

全国计算机技术与软件专业技术资格（水平）考试指定用书

网络规划设计师 2009至2015年试题分析与解答

全国计算机专业技术资格考试办公室 主编

清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试指定用书

网络规划设计师 2009至2015年试题分析与解答

全国计算机专业技术资格考试办公室主编

清华大学出版社
北京

内 容 简 介

网络规划设计师级考试是全国计算机技术与软件专业技术资格（水平）考试的高级职称考试，是历年各级考试报名的热点之一。本书汇集了 2009 下半年至 2015 下半年的所有试题和权威解析，参加考试的考生认真读懂本书的内容后，将会更加了解考题的思路，对提升自己的考试通过率的信心会有极大的帮助。

图书在版编目（CIP）数据

网络规划设计师 2009 至 2015 年试题分析与解答/全国计算机专业技术资格考试办公室主编. —北京：清华大学出版社，2016（2018.1 重印）
（全国计算机技术与软件专业技术资格（水平）考试指定用书）
ISBN 978-7-302-45105-1

Ⅰ. ①网…　Ⅱ. ①全…　Ⅲ. ①计算机网络–资格考试–题解　Ⅳ. ①TP393-44

中国版本图书馆 CIP 数据核字（2016）第 223895 号

责任编辑： 杨如林
封面设计： 何凤霞
责任校对： 胡伟民
责任印制： 沈　露

出版发行： 清华大学出版社
网　　址： http://www.tup.com.cn, http://www.wqbook.com
地　　址： 北京清华大学学研大厦 A 座　　**邮　　编：** 100084
社 总 机： 010-62770175　　**邮　　购：** 010-62786544
投稿与读者服务： 010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈： 010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者： 三河市铭诚印务有限公司
经　　销： 全国新华书店
开　　本： 185mm×230mm　**印　张：** 27.25　**防伪页：** 1　**字　　数：** 665 千字
版　　次： 2016 年 10 月第 1 版　　**印　　次：** 2018 年 1 月第 3 次印刷
印　　数： 4201～5700
定　　价： 69.00 元

产品编号：071279-01

前　言

根据国家有关的政策性文件，全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）已经成为计算机软件、计算机网络、计算机应用、信息系统、信息服务领域高级工程师、工程师、助理工程师、技术员国家职称资格考试。而且，根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，软件设计师、程序员、网络工程师、数据库系统工程师、系统分析师、系统架构设计师和信息系统项目管理师等资格的考试标准已经实现了中国与日本国互认，程序员和软件设计师等资格的考试标准已经实现了中国和韩国互认。

计算机软件考试规模发展很快，年报考规模已超过 30 万人，二十多年来，累计报考人数约 460 多万人。

计算机软件考试已经成为我国著名的 IT 考试品牌，其证书的含金量之高已得到社会的公认。计算机软件考试的有关信息见网站www.ruankao.org.cn中的资格考试栏目。

对考生来说，学习历年试题分析与解答是理解考试大纲的最有效、最具体的途径。

为帮助考生复习备考，全国计算机专业技术资格考试办公室汇集了网络规划设计师 2009 年至 2015 年的试题分析与解答印刷出版，以便于考生测试自己的水平，发现自己的弱点，更有针对性、更系统地学习。

计算机软件考试的试题质量高，包括了职业岗位所需的各个方面的知识和技术，不但包括技术知识，还包括法律法规、标准、专业英语、管理等方面的知识；不但注重广度，而且还有一定的深度；不但要求考生具有扎实的基础知识，还要具有丰富的实践经验。

这些试题中，包含了一些富有创意的试题，一些与实践结合得很好的佳题，一些富有启发性的题，具有较高的社会引用率，对学校教师、培训指导者、研究工作者都是很有帮助的。

由于作者水平有限，时间仓促，书中难免有错误和疏漏之处，诚恳地期望各位专家和读者批评指正，对此，我们将深表感激。

编者

2016 年 6 月

目　　录

第1章　2009下半年网络规划设计师上午试题分析与解答

试题（1）、（2）

在不考虑噪声的条件下，光纤能达到的极限数据率是__（1）__Tbps；光纤上信号在传输过程中有能量损失，工程上在无中继条件下信号在光纤上能传输的最远距离大约是__（2）__千米。

（1）A. 75　　B. 225　　C. 900　　D. 1800

（2）A. 10　　B. 130　　C. 390　　D. 1500

试题（1）、（2）分析

本题考查传输介质和奈奎斯特准则方面的基础知识。

光纤是一种利用光信号运载信息的传输介质。光纤中信号的频率范围约为 10^{14}～10^{15}Hz，按照奈奎斯特准则，其极限数据率可利用公式 $2W\log_2 v$ 计算出来，其中 W 为带宽（频谱宽度）；v 为每个信号所取的离散值数，对通常的光传输，其值为 2，分别表示 1、0。

按照模式的不同，可将光纤简单地分为单模光纤和多模光纤。单模光纤纤芯直径很小，只允许一个模通过，具有更高的数据率，可传输更远的距离，适于长距离通信。光纤衰减系数约为：

850 nm 多模 ＝3 db/km

1300 nm 多模 ＝1 db/km

1300 nm 单模 ＝0.3 db/km

1550 nm 单模 ＝0.2 db/km

可以据此初步估算光纤的传输距离。

按照 ITU-T 的 g.655 规范，采用 1550nm 波长的单模光纤，在 2.5Gbps 条件下的传输距离可达 390km。其他参考值为：

（1）传输速率 1Gbps，850nm。

① 普通 50μm 多模光纤传输距离 550m。

② 普通 62.5μm 多模光纤传输距离 275m。

③ 新型 50μm 多模光纤传输距离 1100m。

（2）传输速率 10Gbps，850nm。

① 普通 50μm 多模光纤传输距离 250m。

② 普通 62.5μm 多模光纤传输距离 100m。

③ 新型 50μm 多模光纤传输距离 550m。

（3）传输速率 2.5Gbps，1550nm。

① g.652 单模光纤传输距离 100km。

② g.655 单模光纤传输距离 390km。

（4）传输速率 10Gbps，1550nm。

① g.652 单模光纤传输距离 60km。

② g.655 单模光纤传输距离 240km。

（5）传输速率 40Gbps，1550nm。

① g.652 单模光纤传输距离 4km。

② g.655 单模光纤传输距离 16km。

参考答案

（1）D （2）C

试题（3）

两个人讨论有关 FAX 传真是面向连接还是无连接的服务。甲说 FAX 显然是面向连接的，因为需要建立连接。乙认为 FAX 是无连接的，因为假定有 10 份文件要分别发送到 10 个不同的目的地，每份文件 1 页长，每份文件的发送过程都是独立的，类似于数据报方式。下述说法正确的是<u>（3）</u>。

（3）A. 甲正确 B. 乙正确 C. 甲、乙都正确 D. 甲、乙都不正确

试题（3）分析

本题考查网络服务的基础知识。

根据传输数据之前双方是否建立连接，可以将网络提供的服务分为面向连接的服务和无连接的服务。面向连接的服务在通信双方进行正式通信之前先建立连接，然后开始传输数据，传输完毕还要释放连接。建立连接的主要工作是建立路由、分配相应的资源（如频道或信道、缓冲区等）。无连接的服务不需要独立地建立连接的过程，而是把建立连接、传输数据、释放连接合并成一个过程一并完成。

FAX 是基于传统电信的一种服务，在发送 FAX 之前需要拨号（即建立连接），拨通并且对方确认接收后开始发送，发送完毕断开连接，因此是面向连接的服务。至于发送 10 份文件，其实是 10 次不同的通信。

参考答案

（3）A

试题（4）

某视频监控网络有 30 个探头，原来使用模拟方式，连续摄像，现改为数字方式，每 5 秒拍照一次，每次拍照的数据量约为 500KB。则该网络<u>（4）</u>。

（4）A. 由电路交换方式变为分组交换方式，由 FDM 变为 TDM

B. 由电路交换方式变为分组交换方式，由 TDM 变为 WDM

C. 由分组交换方式变为电路交换方式，由 WDM 变为 TDM

D. 由广播方式变为分组交换方式，由 FDM 变为 WDM

试题（4）分析

本题考查多路复用方式与交换方式方面的基础知识。

上述视频监控网络因为采用非连续拍照的方式，每次将拍照结果送到监控中心存储，显然是用分组交换方式更恰当。传统的监控是用模拟方式，每个探头连续摄像，一般是用独立线路或使用 FDM 方式传输摄像结果，改用非连续拍照的数字方式后，可以使用 TDM 方式共享传输线路。

参考答案

（4）A

试题（5）

在一个采用 CSMA/CD 协议的网络中，传输介质是一根电缆，传输速率为 1 Gbps，电缆中的信号传播速度是 200 000km/s。若最小数据帧长度减少 800 位，则最远的两个站点之间的距离应至少__（5）__才能保证网络正常工作。

（5）A. 增加 160m　B. 增加 80m　C. 减少 160 m　D. 减少 80 m

试题（5）分析

本题考查 CSMA/CD 的基本原理。

CSMA/CD 要求在发送一帧时如果有冲突存在，必须能在发送最后一位之前检测出冲突，其条件是帧的发送时间不小于信号在最远两个站点之间往返传输的时间。现在帧的长度减少了，其发送时间减少了，因此，为保证 CSMA/CD 能正常工作，最远两个站点之间往返传输的时间必然减少，即电缆长度必然缩短。

设电缆减少的长度为 xm，则信号往返减少的路程长度为 $2x$m，因此有

$2x$ /（200000×1000）$\geqslant$ 800 / 10^9

得到 $x \geqslant 80$。

参考答案

（5）D

试题（6）

局域网 A 为采用 CSMA/CD 工作方式的 10Mbps 以太网，局域网 B 为采用 CSMA/CA 工作方式的 11Mbps WLAN。假定 A、B 上的计算机、服务器等设备配置相同，网络负载大致相同，现在分别在 A、B 上传送相同大小的文件，所需时间分别为 Ta 和 Tb，以下叙述正确的是__（6）__。

（6）A. Ta 大于 Tb　B. Ta 小于 Tb
C. Ta 和 Tb 相同　D. 无法判断 Ta 和 Tb 的大小关系

试题（6）分析

本题考查有线局域网和无线局域网的工作原理及性能。

从 CSMA/CD 的工作原理可知，以太网在发送数据时连续侦测介质，一旦空闲就开

始发送，并且边发送边监听，一旦出现冲突立即停止发送，不需要等待应答就能知道发送操作是否正常完成。而 CSMA/CA 在发现介质空闲时，还要继续等待一个帧间隔（IFS）时间，在发送过程中即使出现冲突，也不能马上知道，需要依靠是否收到对方的有效应答才能确定发送是否正常完成。定性分析的结果，CSMA/CA 成功发送一帧所需要的时间更长。

定量地看，CSMA/CD 方式：帧长=1500B（数据）+18B（帧头）=1518B，发送一帧的时间=1518B/10Mbps=1214μs。CSMA/CA 方式：帧长=1500B（数据）+36B（帧头）=1536B，帧间隔 360μs，帧的发送时间=1536B/11Mbps+360μs ≈1477 μs。假定确认帧很短，其发送时间可忽略，但其等待发送的帧间隔时间不能忽略，则确定一帧正常发送完毕的时间约为 1477+360=1837 μs。所以 CSMA/CA 发送一帧的实际时间明显大于 CSMA/CD 的时间。

参考答案

（6）B

试题（7）

将 10Mbps、100Mbps 和 1000Mbps 的以太网设备互联在一起组成局域网络，则其工作方式可简单概括为<u>（7）</u>。

（7）A. 自动协商，1000Mbps 全双工模式优先
　　B. 自动协商，1000Mbps 半双工模式优先
　　C. 自动协商，10Mbps 半双工模式优先
　　D. 人工设置，1000Mbps 全双工模式优先

试题（7）分析

本题考查以太网设备及以太网协议方面的基本知识。

10Mbps、100Mbps 和 1000Mbps 以太网设备（主要指交换机、网卡等）互联在一起时，自动协商其传送速率，确定的顺序是依次从最高到最低，同一速率下的协商顺序是先全双工后半双工。

参考答案

（7）A

试题（8）

规划师在规划 VLAN 时，用户向其提出将用户的一台计算机同时划分到两个不同的 VLAN。规划师的解决方案是<u>（8）</u>。

（8）A. 告诉用户这一要求不能满足
　　B. 将用户计算机所连接的交换机端口设置成分属两个不同的 VLAN，因为交换机都支持这种方式
　　C. 在用户计算机上安装两个网卡，分别连接到不同的交换机端口，设置成各属于一个 VLAN

D. 让网络自动修改 VLAN 配置信息，使该用户的计算机周期性地变更所属的 VLAN，从而连接到两个不同的 VLAN

试题（8）分析

本题考查虚拟局域网方面的基本知识。

通常情况下，将普通计算机分属不同的 VLAN，事实上导致安全隐患，因为该计算机成为一个跨 VLAN 访问的桥。但特定的计算机需要分属不同 VLAN，例如数据库服务器、邮件服务器等，通常是被所有用户共享的，这就需要让不同 VLAN 上的计算机都能访问。

实现上述目标的基本方法是在该计算机上安装两个网卡，分别连接到不同的交换机端口，设置成各属于一个 VLAN。

现在有一些交换机，支持将一个端口设置成分属不同的 VLAN，这样就更简单，但并不是所有的交换机都具有这一功能。

参考答案

（8）C

试题（9）

某应用通过一个广域网传输数据，每次所传输的数据量较小，但实时性要求较高，网络所处的环境干扰信号比较强，则为该网络选择的工作方式应为__（9）__。

（9）A. 永久虚电路方式　　B. 临时虚电路方式
C. 数据报方式　　D. 任意

试题（9）分析

本题考查广域网的实现方法。

数据报方式对每个分组都单独选择路由，而临时虚电路（常简称为虚电路）方式是对每次通信都建立一条路由，该次通信的多个分组都经由同一条路径传送。虚电路方式适于数据量较大、出错率较低、实时性要求不高的场合，因为建立虚电路的开销较大，一旦建立虚电路后，如果只传送很少的数据（比如一个分组），则总的效率很低。同时，虚电路一旦建立，所有数据都经同一路径传送，如果出错率很高，则可能导致中途失败，需要重新建立虚电路、重新传送，极端情况下，无法成功传送数据。相反，数据报方式由于每个分组都独立地传送，有可能每个分组都是经最佳路由到达目的地，所以更适于数据量较小（通常一个分组）、出错率较高、实时性要求较高的场合。

参考答案

（9）C

试题（10）

距离向量路由算法是 RIP 路由协议的基础，该算法存在无穷计算问题。为解决该问题，可采用的方法是每个节点__（10）__。

（10）A. 把自己的路由表广播到所有节点而不仅仅是邻居节点
B. 把自己到邻居的信息广播到所有节点

C. 不把从某邻居节点获得的路由信息再发送给该邻居节点

D. 都使用最优化原则计算路由

试题（10）分析

本题考查路由算法与路由协议方面的基本知识。

导致无穷计算问题的一个重要原因是把从对方获知的，但在对方已不再有效的信息当成有效信息再传送给对方，使对方当成有效信息使用。因此只要不把从某邻居节点获得的路由信息再发送给该邻居节点，就能基本上避免无穷计算问题。

参考答案

（10）C

试题（11）

SDH 网络通常采用双环结构，其工作模式一般为（11）。

（11）A. 一个作为主环，另一个作为备用环，正常情况下只有主环传输信息，在主环发生故障时可在 50ms 内切换到备用环传输信息

B. 一个作为主环，另一个作为备用环，但信息在两个环上同时传输，正常情况下只接收主环上的信息，在主环发生故障时可在 50ms 内切换到从备用环接收信息

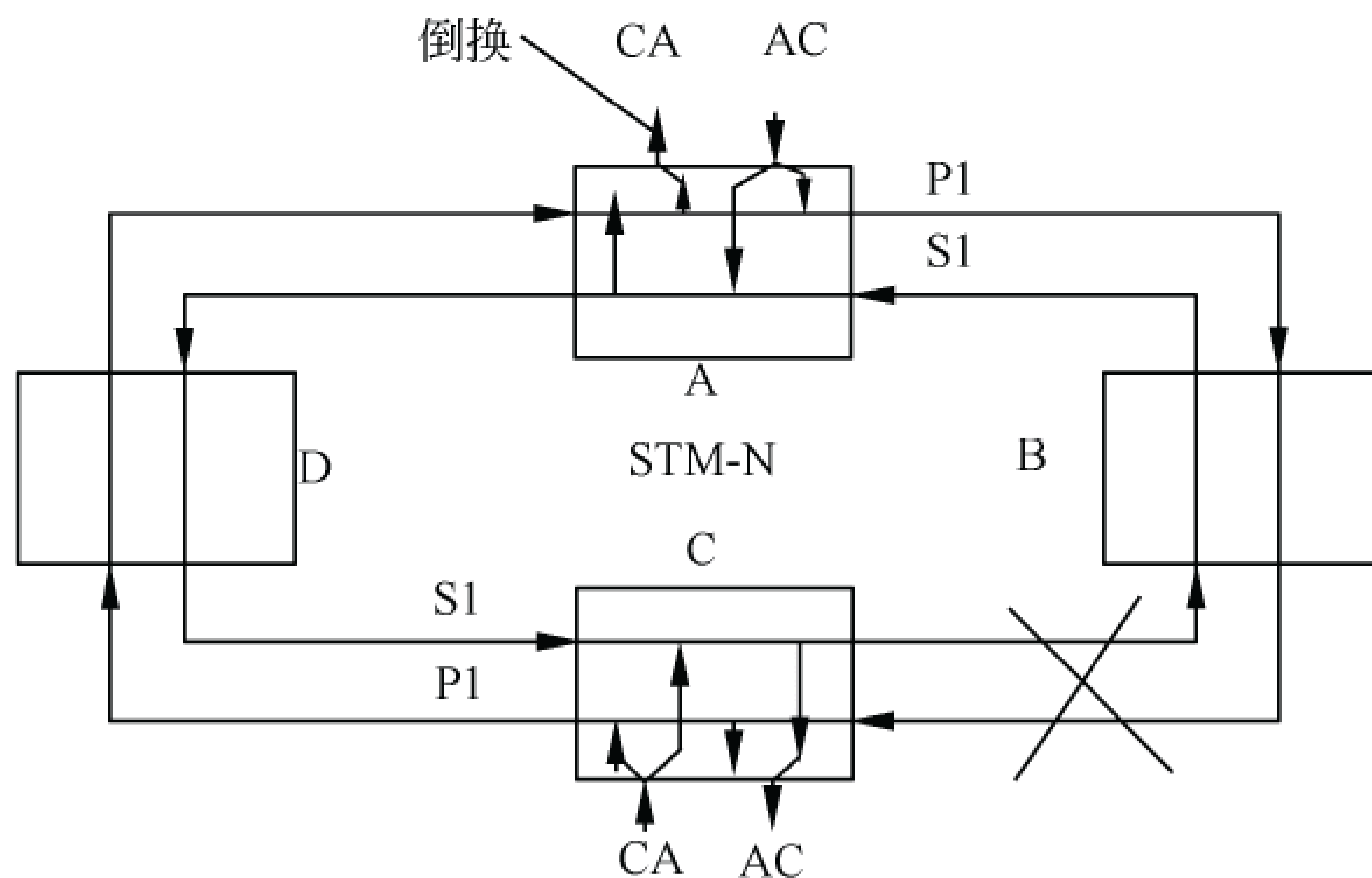
C. 两个环同时用于通信，其中一个发生故障时，可在 50ms 内屏蔽故障环，全部信息都经另一个环继续传输

D. 两个环同时用于通信，任何一个发生故障时，相关节点之间的通信不能进行，等待修复后可在 50ms 内建立通信连接继续通信

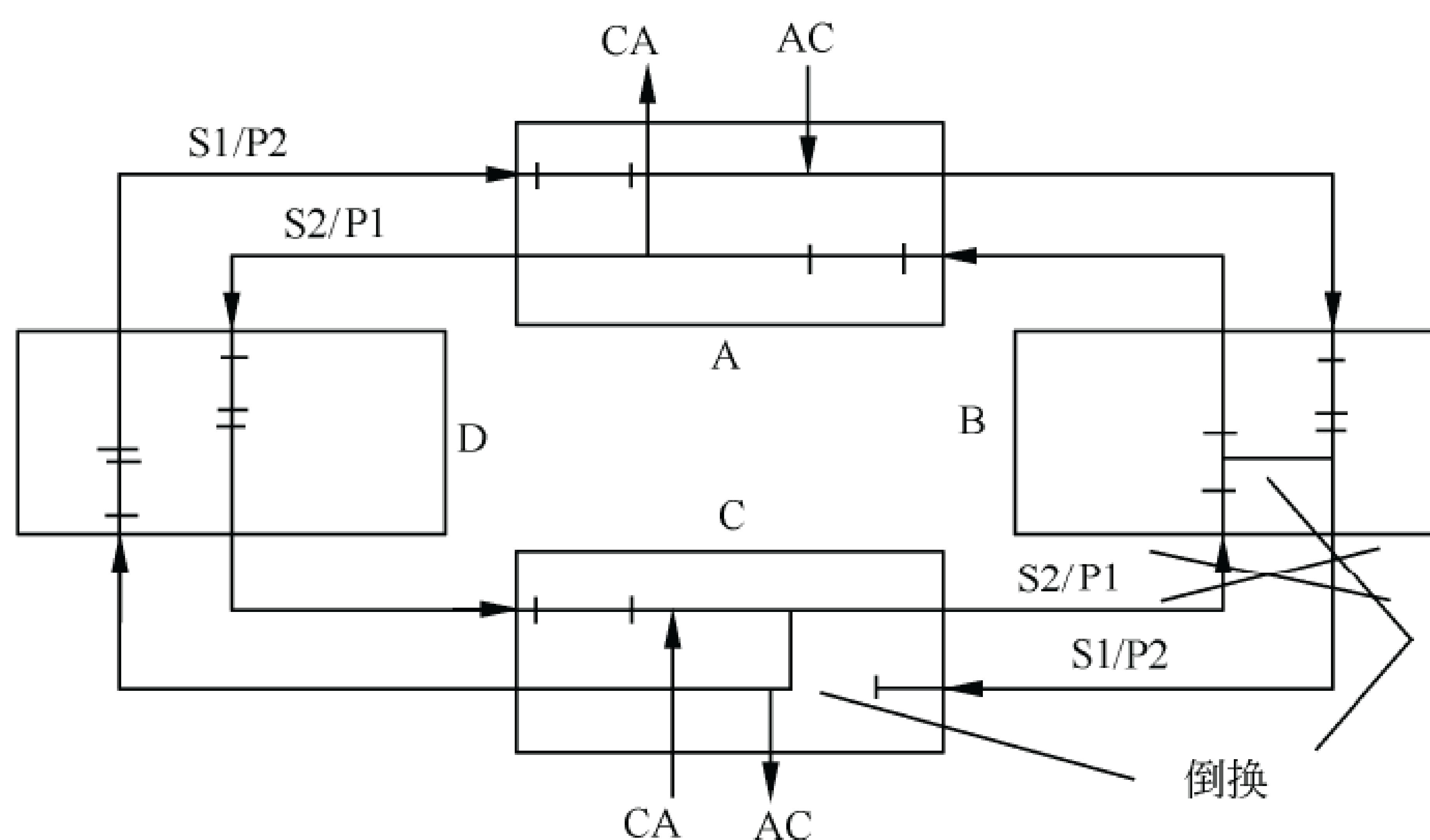
试题（11）分析

本题考查广域网中 SDH 网络的基本知识。

SDH 网络具有链型、星型、环型、树型和网孔型等结构形式，其中双环结构是一种常用的形式，因为其具有自愈功能，能提供较高的可靠性。较常用的有双纤单向通道保护环和双纤双向复用段保护环，其结构如下图所示。



双纤单向通道保护环示意图



双纤双向复用段保护环示意图

参考答案

（11）B

试题（12）

ADSL 是个人用户经常采用的 Internet 接入方式，以下关于 ADSL 接入的叙述，正确的是__（12）__。

（12）A. 因使用普通电话线路传输数据，所以电话线路发生故障时，可就近换任一部电话的线路使用，且最高可达 8Mbps 下行、1Mbps 上行速率

B. 打电话、数据传输竞争使用电话线路，最高可达 8Mbps 下行、1Mbps 上行速率

C. 打电话、数据传输使用 TDM 方式共享电话线路，最高可达 4Mbps 下行、2Mbps 上行速率

D. 打电话、数据传输使用 FDM 方式共享电话线路，最高可达 8Mbps 下行、1Mbps 上行速率

试题（12）分析

本题考查接入网中 ADSL 接入技术的基本知识。

ADSL 技术将语音电话和网络数据调制到不同频段，采用 FDM 方式在一对电话线上传输。

参考答案

（12）D

试题（13）、（14）

设计一个网络时，分配给其中一台主机的 IP 地址为 192.55.12.120，子网掩码为 255.255.255.240。则该主机的主机号是__（13）__；可以直接接收该主机广播信息的地址范围是__（14）__。

（13）A. 0.0.0.8　　B. 0.0.0.120　　C. 0.0.0.15　　D. 0.0.0.240

（14）A. 192.55.12.120～192.55.12.127

B. 192.55.12.112～192.55.12.127

C. 192.55.12.1～192.55.12.254

D. 192.55.12.0～192.55.12.255

试题（13）、（14）分析

本题考查 IP 地址的基本知识。

IP 地址由网络地址和主机地址两部分构成，主机地址可进一步划分为子网号和主机号两部分，三者的区分需借助子网掩码实现。

主机号是 IP 地址中去掉网络地址、子网号后的部分，其计算方法可简单利用公式“主机号=IP 地址 AND（NOT（子网掩码））”计算。

一台计算机发出的广播消息，只有处在同一子网（网络）内的计算机才能接收到。192.55.12.120 的子网（网络）地址=IP 地址 AND 子网掩码=（192.55.12.120 AND 255.255.255.240）=192.55.12.112，IP 地址的最后 4 位为主机号，范围为 0～15，加在子网号后面即可。

参考答案

（13）A　　（14）B

试题（15）

在一个网络内有很多主机，现在需要知道究竟有哪些主机。方法之一是：从指定网络内的第一个主机地址开始，依次向每个地址发送信息并等待应答。该方法所使用的协议及报文是__（15）__。

（15）A. ICMP，回送请求报文

B. UDP，17 类型报文

C. TCP，SYN 报文

D. PING，测试报文

试题（15）分析

本题考查 ICMP 协议的基本内容。

ICMP 协议有很多功能，其中之一是向指定主机发送回送请求报文，对方收到后会发送一个应答报文，报告自己的状态。PING 应用就是利用这一功能实现的。

参考答案

（15）A

试题（16）

在 IPv6 中，一个节点可以为自己自动配置地址，其依据的主要信息是__（16）__。

（16）A. 网卡的 MAC 地址

B. 前一次配置的 IPv6 地址

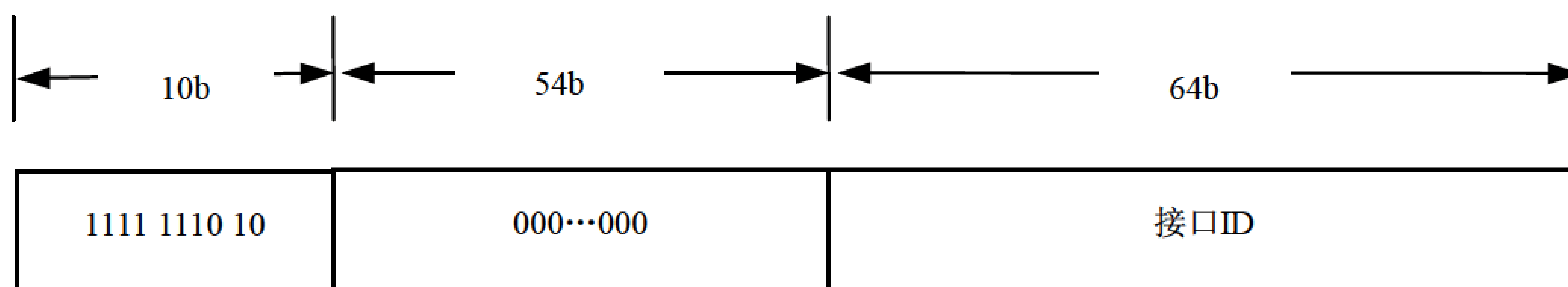
C. 推测 DHCP 可能分配的 IPv6 地址

D. 任意选择的一个 IPv6 地址

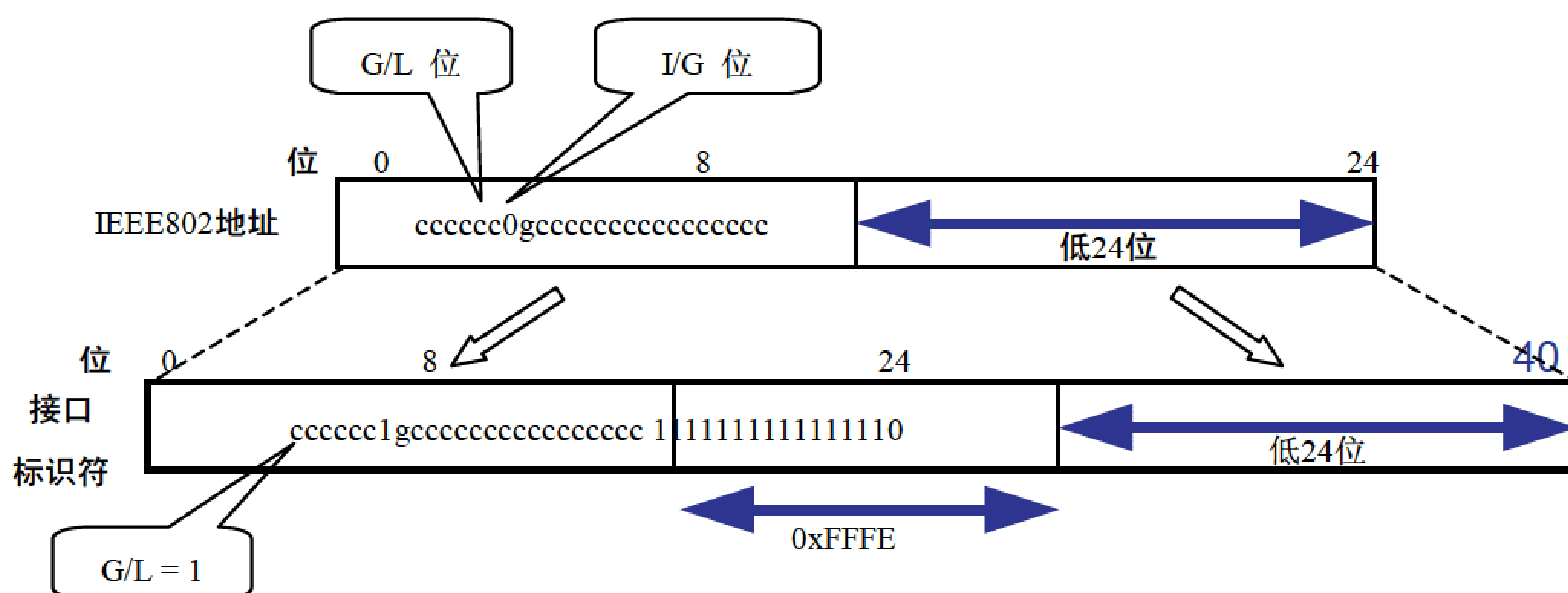
试题（16）分析

本题考查 IPv6 的基本内容。

IPv6 自动配置的地址主要是本地单播地址，其格式为：



其中接口 ID 根据网卡的 MAC 地址自动生成，生成方式为：



参考答案

（16）A

试题（17）

TCP 使用慢启动拥塞避免机制进行拥塞控制。当前拥塞窗口大小为 24，当发送节点出现超时未收到确认现象时，将采取的措施是＿（17）＿。

（17）A. 将慢启动阈值设为 24，将拥塞窗口设为 12

B. 将慢启动阈值设为 24，将拥塞窗口设为 1

C. 将慢启动阈值设为 12，将拥塞窗口设为 12

D. 将慢启动阈值设为 12，将拥塞窗口设为 1

试题（17）分析

本题考查 TCP 协议的拥塞控制方法。

TCP 的慢启动拥塞避免机制调整慢启动阈值和拥塞窗口的方法是：当出现超时未收

到确认的现象时，判定为出现了拥塞（至少是具有拥塞的征兆），并将慢启动阈值设为当前拥塞窗口的一半，将拥塞窗口设为 1，继续慢启动过程。

参考答案

（17）D

试题（18）

NAT 是实现内网用户在没有合法 IP 地址情况下访问 Internet 的有效方法。假定内网上每个用户都需要使用 Internet 上的 10 种服务（对应 10 个端口号），则一个 NAT 服务器理论上可以同时服务的内网用户数上限大约是<u>（18）</u>。

（18）A. 6451　　B. 3553　　C. 1638　　D. 102

试题（18）分析

本题考查 NAT 的基本原理。

NAT 服务器需要建立一张对照表，记录内部地址。其方法是对每个内部地址及请求的服务（端口号）分配一个新的端口号，作为转换后报文的源端口号（源地址为 NAT 服务器所具有的合法 IP 地址）。由于端口号总数只有 65 536 个，而 0～1023 的端口号为熟知端口不能随意重新定义，因此可供 NAT 分配的端口号大约为 64 512 个。因为每个内网用户平均需要 10 个端口号，所以能容纳的用户数（机器数）约为 6451。

参考答案

（18）A

试题（19）

具有断点续传功能的 FTP 客户端软件，在续传时需要与 FTP 服务器交换断点的位置信息，以下叙述正确的是<u>（19）</u>。

（19）A. 断点位置信息存放在客户端，通过数据连接告诉 FTP 服务器
B. 断点位置信息存放在客户端，通过控制连接告诉 FTP 服务器
C. 断点位置信息存放在服务器端，通过数据连接告诉 FTP 客户端
D. 断点位置信息存放在服务器端，通过控制连接告诉 FTP 客户端

试题（19）分析

本题考查 FTP 的基本知识。

FTP 需要在客户端与服务器之间建立两个连接：控制连接和数据连接，分别传送控制信息和文件内容。断点续传是对传统 FTP 的改进，使得在因某种原因中断传输并再次启动传输时，可以接着传输，而不必从头开始重传。其中断点信息保存在客户端上（FTP 客户端软件完成断点的保存与读取）。

参考答案

（19）B

试题（20）

为了在不同网页之间传递参数，可以使用的技术及其特性是<u>（20）</u>。

（20）A. Cookie，将状态信息保存在客户端硬盘中，具有很高的安全性
B. Cookie，将状态信息保存在服务器硬盘中，具有较低的安全性
C. Session，将状态信息保存在服务器缓存中，具有很高的安全性
D. Session，将状态信息保存在客户端缓存中，具有较低的安全性

试题（20）分析

本题考查 HTTP 协议的基本知识及其应用。

在不同网页之间传递参数，常见的有 4 种方法：Cookie、Session、数据库和 Ajax。其中 Cookie 方法将参数保存在客户端硬盘中（存在安全性问题），Session 将参数保存在服务器缓存中（数据量受限），数据库方法将参数保存在数据库中（数据的结构化问题及速度问题），Ajax 方法以局部更新页面的方式实现参数的传递。

参考答案

（20）C

试题（21）、（22）

网络管理功能使用 ASN.1 表示原始数据，整数 49 使用 ASN.1 表示的结果是（21）；SNMP 协议的 GetBulkRequest 一次从设备上读取的数据是（22）。

（21）A. 49　　B. 2，1，49　　C. 206　　D. 2，49

（22）A. 一条记录　　B. 连续多条记录
C. 受 UDP 报文大小限制的数据块　　D. 所要求的全部数据

试题（21）、（22）分析

本题考查 SNMP 协议、管理数据的表示及 ASN.1 的基本知识。

ASN.1 表示数据的方法简称为 TLV 表示法，主要由标记（Tag）、长度（Length）和值（Value）三部分构成。“标记”标明数据的类型，1 个字节，由 2 位类别、1 位格式和 5 位类型序号组成。“长度”标明数据的长度（通常是指字节数），数据长度小于 128 字节时，长度字段为一个字节；否则为多个字节，前面字节的高位为 1，最后一个字节的高位为 0。“值”标明数据的具体值，整数用 2 的补码表示，位串直接编码，但前面加一个字节表示最后一个字节中未用的位数。

GetBulkRequest 是 SNMPv2 用于快速读取被管设备上数据的方法，一次能读多条连续的记录，长度受 UDP 报文长度的限制。

参考答案

（21）B　（22）C

试题（23）、（24）

传统的 Internet 提供的是没有 QoS 保证的、尽力而为的服务。其实在 IPv4 包中已经定义了服务类型字段，包括优先级、吞吐量、延迟、可靠性等，只要（23）处理该字段，就可提供 QoS 保证。MPLS 是一种更通用的 QoS 保证机制，其基本思想可简述为（24）。

（23）A. 交换机　B. 路由器　C. 服务器　D. 客户端

（24）A. 标记交换路由器为 IP 分组加上标记，其他路由器按优先级转发

B. 边缘路由器对业务流进行分类并填写标志，核心路由器根据分组的标志将其放入不同的队列转发

C. 在建立连接时根据优先级预留所需要的资源以提供所要求的 QoS

D. 根据 IP 分组中自带的优先级信息对 IP 分组进行排队，保证高优先的分组优先转发

试题（23）、（24）分析

本题考查 Internet 服务质量的基本知识。

在 IP 协议的早期版本中定义了一个服务类型字段（1 字节），内容为 PPPDTR00，其中 PPP 定义优先级，D 为延迟，T 为吞吐量，R 为可靠性。D、T、R 的值取 0 表示低，取 1 表示高。但遗憾的是，路由器都未处理该字段，导致 IP 不能提供 QoS。1998 年，该字段被更名为区分服务，以提供 DiffServ 服务。

MPLS 是一种应用更广泛的 QoS 方案，其基本思想可简述为：标记交换路由器（通常在网络的边缘）为 IP 分组加上标记，其他路由器根据分组中的标记按优先级转发，从而实现 QoS 服务。

参考答案

（23）B　（24）A

试题（25）、（26）

某机构拟建设一个网络，委托甲公司承建。甲公司的赵工程师带队去进行需求调研，在与委托方会谈过程中记录了大量信息，经过整理，归纳出如下主要内容：

用户计算机数量：97 台；业务类型：办公；连接 Internet：需要；分布范围：分布在一栋楼房的三层内（另附位置图一张）；最远距离：78 米；需要的网络服务：邮件、Web；网络建设时间：三个月。

在撰写需求分析报告时，发现缺少了一些很重要的信息，其中包括 （25） 。为此，赵工再次与委托方进行交谈，获得所需信息后，开始撰写需求分析报告。该报告的目录如下：一、业务需求；二、用户需求；三、应用需求；四、计算机需求；五、网络需求；六、使用方式需求；七、建设周期；八、经费预算。关于该报告的评价，恰当的是 （26） 。

（25）A. 估计的通信量　B. 计算机的性能

C. 经费预算　D. 应用系统的运行平台

（26）A. 使用方式需求应合并到业务需求或用户需求中

B. 应用需求应合并到业务需求中

C. 经费预算部分应删除

D. 是一个比较好的报告无需调整

试题（25）、（26）分析

本题考查网络规划与设计中需求分析的相关知识。

在需求分析阶段，至少应了解业务需求、用户需求、应用需求、平台需求和网络需求等基本信息，其中通信量分析是业务需求的重要组成部分。

需求分析报告应包括对技术方面的详细描述，另外包括对建设周期等非技术性内容的描述，一般不需要描述经费预算，因为经费是非常敏感、在招标完成前可能需要保密的信息。当然，经费与建设内容并不能完全分离，如果预算少，建设内容事实上不可能完成。很多情况下是根据需求来确定经费预算。

参考答案

（25）A　　（26）C

试题（27）～（29）

甲公司承接了乙公司的网络建设工作。由于待建网络规模很大，为确保建设工作顺利进行，负责该项目的工程师在进行逻辑设计时提出了如下工作思路：

① 明确逻辑设计工作的内容是：网络拓扑结构设计；物理层技术选择；局域网技术选择；广域网技术选择；地址设计；路由协议选择；网络管理模式与工具选择；撰写逻辑设计文档。

② 在进行地址设计时，确定的方案是：按乙公司各分支机构的地理位置划分地址块，并按 10 . n . X .Y /16 的模式分配，其中 n 为分支机构的序号（0 表示公司总部，分支机构总数不会超过 200）。

对该工程师确定的逻辑设计内容的评价，恰当的是<u>（27）</u>。

每个分支机构能连网的计算机的数量最多为<u>（28）</u>，配置 IP 地址时掩码是<u>（29）</u>。

（27）A. 内容全面，符合逻辑设计的工作准则
B. 应去掉物理层技术选择这一部分
C. 应去掉路由协议选择这一部分
D. 应增加网络安全设计这一部分

（28）A. 16　　B. 256　　C. 65534　　D. 65536

（29）A. 255.0.0.0　　B. 255.255.0.0　　C. 255.255.255.0　　D. 255.255.240.0

试题（27）～（29）分析

本题考查逻辑网络设计的相关知识。

逻辑网络设计应完成的主要设计包括网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理方案设计和网络安全方案设计。

采用 10 . n . X .Y /16 的地址模式，每个机构可以用 16 位作为机构内的主机地址（去掉全 0、全 1 的地址）。

参考答案

（27）D （28）C （29）B

试题（30）、（31）

在一个 16 000 m^2 建筑面积的八层楼里，没有任何现成网线，现有 1200 台计算机需要连网，对网络的响应速度要求较高，同时要求 WLAN 覆盖整栋楼满足临时连网的需要。设计师在进行物理网络设计时，提出了如下方案：设计一个中心机房，将所有的交换机、路由器、服务器放置在该中心机房，用 UPS 保证供电，用超 5 类双绞线电缆作为传输介质，在每层楼放置一个无线 AP。该设计方案的致命问题之一是<u>（30）</u>，其他严重问题及建议是<u>（31）</u>。

（30）A. 未计算 UPS 的负载
B. 未明确线路的具体走向
C. 交换机集中于机房浪费大量双绞线电缆
D. 交换机集中于机房使得水平布线超过 100m 的长度限制

（31）A. 每层一个 AP 不能实现覆盖，应至少部署三个 AP
B. 只有一个机房，没有备份，存在故障风险，应设两个机房
C. 超 5 类双绞线性能不能满足要求，应改用 6 类双绞线
D. 没有网管系统，应增加一套网管系统

试题（30）、（31）分析

本题考查物理网络设计的相关知识。

进行物理网络设计时需要有准确的地形图、建筑结构图，以便规划线路走向、计算传输介质的数量，评估介质布设的合理性。

8 层楼 16 000m^2，每层楼 2000m^2，相当于 20×100（或 40×50）m 的布局。可以明显看出，将全部交换机置于中心机房、使用超 5 类 UTP，很多线的长度超过 100m，违反布线规定，将导致网络不能正常工作。

同时，每层部署一个 AP，显然不能很好地全覆盖。因为在楼内 AP 的覆盖范围很小，有时只有 20～30m，甚至更小。

参考答案

（30）D （31）A

试题（32）、（33）

设计师制定的网络测试计划中，连通性测试方案是：利用测试工具对每个设备和信息点进行 3 次 Ping 测试，如果 3 次都显示连通，即判定该点为连通。链路速率测试方案是：用 2 台测试设备分别接在每根线路的两端，一台以 100Mbps 速率发送，另一台接收，接收速率不低于发送速率的 99%即判定合格。对连通性测试方案的评价，恰当的是<u>（32）</u>，对链路速率测试方案的评价，恰当的是<u>（33）</u>。

（32）A. 是一个标准的方案

B. 应测试响应时间
C. 应测试 10 次且必须每次都是连通的
D. 只需测试信息点，不用测试网络设备

（33）A. 是一个标准的方案
B. 应该多测试几种速率
C. 应该将 2 台测试设备分别连接到包含交换机等设备的网络上而不是单根线路上
D. 接收速率与发送速率相同才能判定为合格

试题（32）、（33）分析

本题考查网络的测试、优化和管理方面的基本知识。

网络测试没有现成的标准，通常是一些经验的总结和行业的通用做法。比如连通性测试，一般是连续测试 10 次以上。

对速率的测试，应测试端到端的速率，而不是路径段的速率。

参考答案

（32）C （33）C

试题（34）、（35）

某园区有多栋房屋，每栋房屋都通过光缆连接到机房的同一设备上，现在其中一栋房屋内的用户不能访问 Internet，引起这一故障现象的原因首先应判断为__（34）__，采取相应措施后，故障依然存在，此时最可能的问题是__（35）__。

（34）A. 机房网络设备故障
B. DNS 服务器故障
C. 网络配置变更
D. 该栋房屋到机房的光缆故障

（35）A. 该栋楼房的光终端设备损坏
B. 用户机器的协议配置错误
C. VLAN 配置错误
D. DHCP 服务器故障

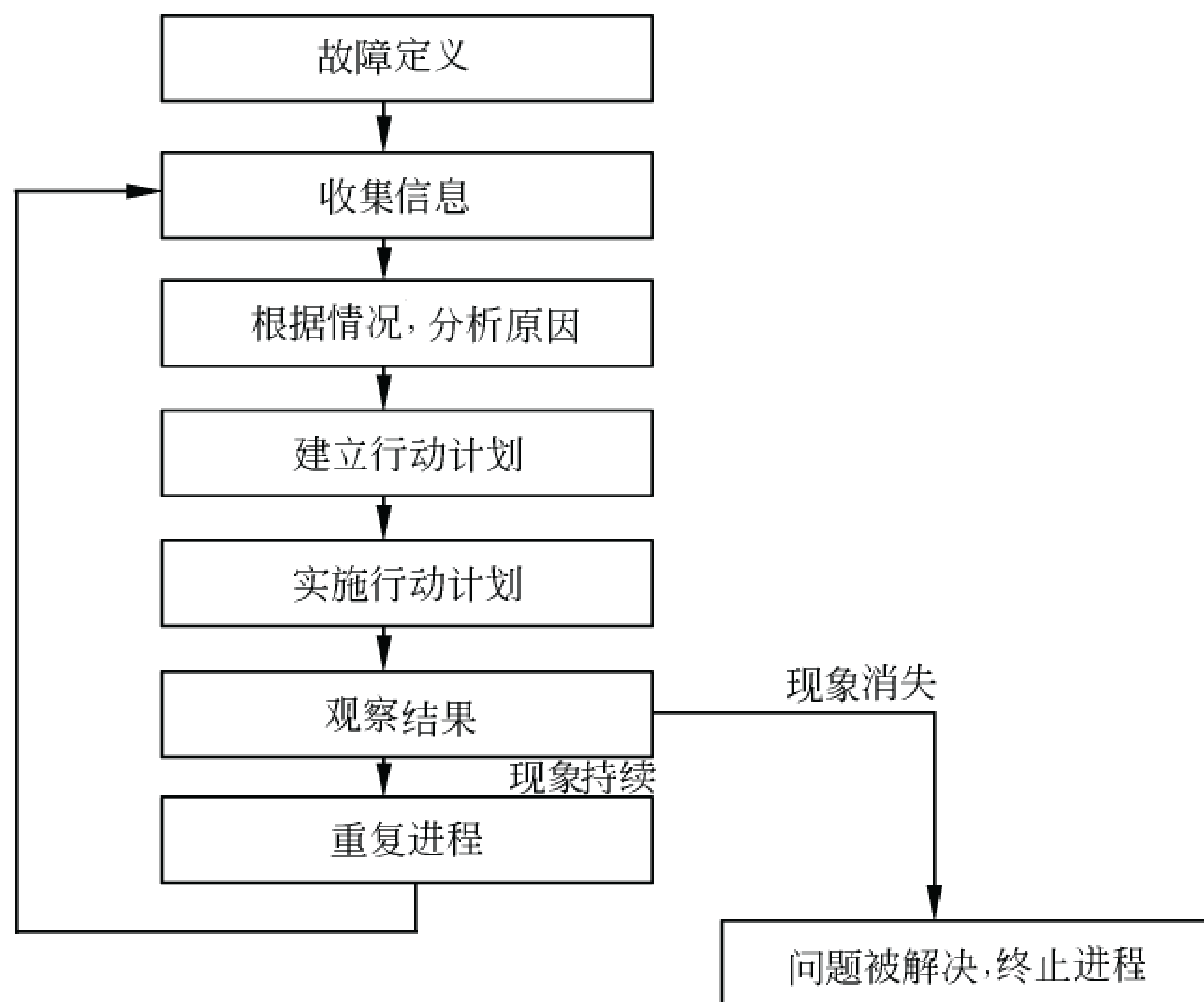
试题（34）、（35）分析

本题考查网络故障分析与处理方面的基本知识。

网络故障分析与处理的一般思路是：

故障分析与处理模型。其中原因分析、制定行动方案没有标准的模式，在很大程度上依赖人的知识和经验，包括对各类设备、介质和软件等的了解。

针对本题的现象，首先会设想该栋楼房到机房的光纤出现问题（被弄断了）。如果光纤没问题，因机房的设备工作正常，所以下一个怀疑对象就应该是该栋楼的光端设备出现故障。



参考答案

（34）D　　（35）A

试题（36）、（37）

对网络性能进行评估时，需要明确的主要性能指标是__（36）__，除了可用理论方法进行分析外，更多地需要进行实际测量，主要的测量方法是__（37）__。

（36）A. 实际数据率　　B. 丢包率
C. 延迟时间　　D. 延迟抖动

（37）A. 用速率测试仪，测试线路速率
B. 运行测试程序，发送大量数据，观察实际性能值
C. 收集网络上传输过程的全部信息，进行分析
D. 将用户程序放在不同网络上运行，比较所需时间

试题（36）、（37）分析

本题考查网络性能评估方面的基本知识。

网络性能应以用户获得的实际性能为准，而不是以理论数据为准，因此一般方法是运行各种测试软件或实际应用系统，观察实际的性能数据，与理论值进行对比分析，据此作出评估。

参考答案

（36）A　　（37）B

试题（38）、（39）

为数据库服务器和 Web 服务器选择高性能的解决方案，较好的方案是__（38）__，其原因在于__（39）__。

（38）A. 数据库服务器用集群计算机，Web 服务器用 SMP 计算机
B. 数据库服务器用 SMP 计算机，Web 服务器用集群计算机
C. 数据库服务器和 Web 服务器都用 SMP 计算机
D. 数据库服务器和 Web 服务器都用集群计算机

（39）A. 数据库操作主要是并行操作，Web 服务器主要是串行操作
B. 数据库操作主要是串行操作，Web 服务器主要是并行操作
C. 都以串行操作为主
D. 都以并行操作为主

试题（38）、（39）分析

本题考查重要的网络资源设备——网络服务器的有关知识。

高性能服务器主要有 SMP 结构、MPP 结构、集群结构和 Constellation 结构。

数据库管理系统主要是串行处理，因选用适宜进行高速串行运算的服务器，所以应选用 SMP 结构的服务器。

Web 服务器同时为很多用户服务，且各自请求的内容没有关联性，可完全并行化处理，因此选用全并行的、集群结构的服务器。

参考答案

（38）B　　（39）B

试题（40）、（41）

用户针对待建设的网络系统的存储子系统提出的要求是：存取速度快、可靠性最高、可进行异地存取和备份，则首选方案是<u>（40）</u>，其中硬盘系统应选用<u>（41）</u>。

（40）A. NAS　B. DAS　C. IP SAN　D. FC SAN

（41）A. RAID 0　B. RAID 1　C. RAID 5　D. RAID 6

试题（40）、（41）分析

本题考查存储系统方面的基本知识。

存储系统的主要结构有三种：NAS、DAS 和 SAN。

DAS（Direct Attached Storage，直接附加存储）存储设备是通过电缆（通常是 SCSI 接口电缆）直接连接服务器，I/O 请求直接发送到存储设备。DAS 也可称为 SAS（Server-Attached Storage，服务器附加存储），它依赖于服务器，其本身是硬件的堆叠，不带有任何存储操作系统。

DAS 的适用环境为：（1）服务器在地理分布上很分散，通过 SAN（存储区域网络）或 NAS（网络直接存储）在它们之间进行互连非常困难时；（2）存储系统必须被直接连接到应用服务器（如 Microsoft Cluster Server 或某些数据库使用的“原始分区”）上时；（3）包括许多数据库应用和应用服务器在内的应用，它们需要直接连接到存储器上时。

NAS（Network Attached Storage，网络附加存储）存储系统不再通过 I/O 总线附属于某个特定的服务器或客户端，而是直接通过网络接口与网络相连，由用户通过网络来访

问。NAS 实际上是一个带有瘦服务的存储设备，其作用类似于一个专用的文件服务器，不过把显示器、键盘和鼠标等设备省去。NAS 用于存储服务，可以大大降低存储设备的成本。另外，NAS 中的存储信息都是采用 RAID 方式进行管理的，从而可有效地保护数据。用户访问 NAS 同访问一台普通计算机的硬盘资源一样简单，甚至可以通过设置 NAS 设备为一台 FTP 服务器，这样其他用户就可以通过 FTP 访问 NAS 中的资源了。也可以通过网页浏览的方式对 NAS 进行管理。

SAN（Storage Area Network，存储区域网络）是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统。SAN 主要采取数据块的方式进行数据存储，目前主要有 IP SAN 和 FC SAN 两种形式（分别使用 IP 协议和光纤通道）。通过 IP 协议，能利用廉价、货源丰富的以太网交换机、集线器和线缆实现低成本、低风险基于 IP 的 SAN 存储。光纤通道是一种存储区域网络技术，它实现了主机互连，企业间共享存储系统的需求。可以为存储网络用户提供高速、高可靠性以及稳定安全性的传输。光纤通道是一种高性能、高成本的技术。

RAID（独立磁盘冗余阵列）是一种把多块独立的硬盘（物理硬盘）按不同的方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能和提供数据备份的技术。常见的有 RAID 0、RAID 1、RAID 5 和 RAID 10（即 RAID 1+0）等实现方式。RAID 0 把多个磁盘变成一个逻辑磁盘使用，主要是扩大容量。RAID 1 是把两个磁盘做成热备份。RAID 5 至少需要 3 个硬盘，对每个数据块进行校验，把校验信息单独存储，一旦原始数据的存储位置发生故障，可通过校验信息恢复丢失的信息。RAID 5 的有效存储容量约为磁盘总存储容量的 1/3。RAID 10 是把 RAID 0 和 RAID 1 结合使用。

参考答案

（40）C　　（41）B

试题（42）、（43）

某用户是一个垂直管理的机构，需要建设一个视频会议系统，基本需求是：一个中心会场，18 个一级分会场，每个一级分会场下面有 3～8 个二级分会场，所有通信线路为 4Mbps，主会场、一级分会场为高清设备，可在管辖范围内自由组织各种规模的会议，也可在同级之间协商后组织会议，具有录播功能。（42）不是中心会场 MCU 设备应具备的规格或特点，（43）不是中心会场录播设备应具备的规格或特点。

（42）A. 支持 H.323 协议
B. 支持 H.261/H.263/H.263+/H.264 视频编码格式
C. 支持 CIF/4CIF/720P 视频格式
D. 支持 G.711/G.722.1 Annex C /G.728/G.729/MPEG4-AAC（LC/LD）音频格式

（43）A. 支持实时数字录制和在线点播功能
B. 支持 H.261/H.263/H.263+/H.264/MPEG-4 视频编码格式
C. 可录制 CIF/4CIF/720P/1080i/1080P 等视频格式会议

D. 可对主会场进行录像并支持 20 路同时点播

试题（42）、（43）分析

本题考查网络应用资源——视频会议系统的基本知识。

满足上述需求的中心会场 MCU 一般具有较高的性能、较好的兼容性、可扩展性。现在所说的高清都是指 1080 线以上，所以 720P 没有满足用户需求。

主会场的录播设备应能对一级分会场进行录播。

参考答案

（42）C （43）D

试题（44）、（45）

应用 MPLS VPN 转发数据包时，所依据的信息是__（44）__，在 MPLS VPN 中用户使用专用的 IP 地址，因此__（45）__。

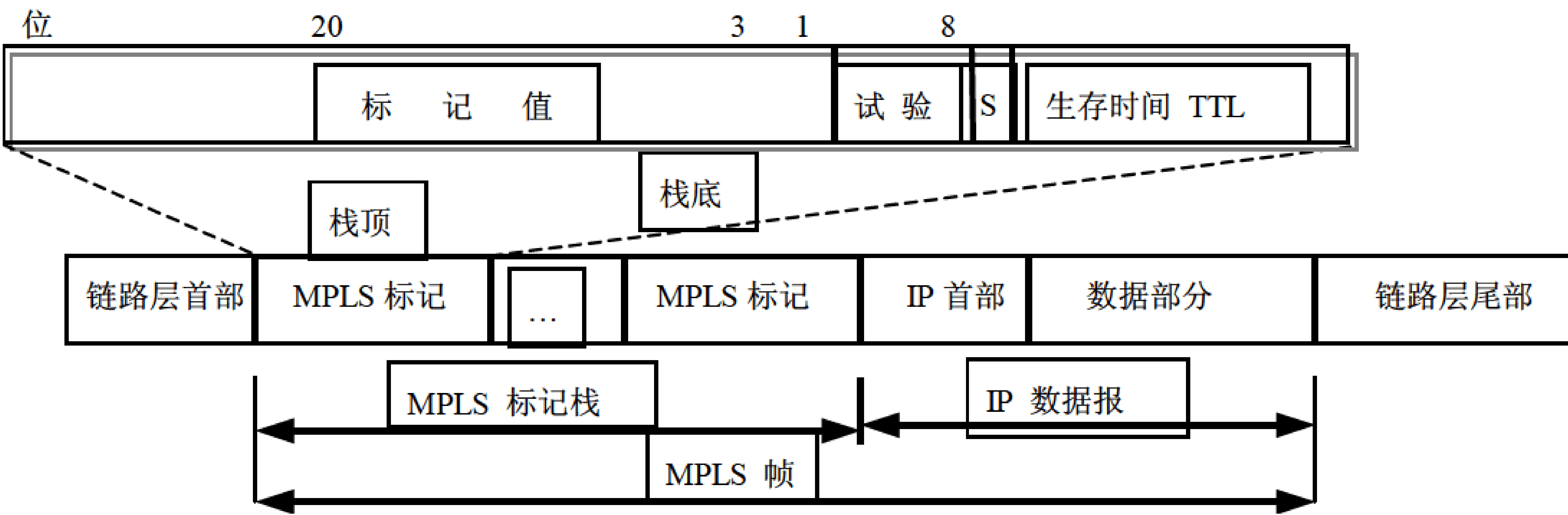
（44）A. VPN 标识符+IP 地址
B. VPN 标识符
C. IP 地址
D. IP 地址+掩码

（45）A. 当用户需要访问 Internet 时，需要有 NAT
B. 无需 NAT，因用户只能与 VPN 成员通信
C. 所谓的专用地址必须是 Internet 上合法的 IP 地址
D. 专用地址可由 VPN 标识符推算出来

试题（44）、（45）分析

本题考查 VPN 的相关知识。

MPLS VPN 的基本原理是：MPLS 域边界路由器在 IP 包之前添加 MPLS 标记组成 MPLS 帧，再按所使用的 VPN 协议封装成相应的 VPN 帧，按 VPN 模式传送。其帧格式如下图所示。



MPLS VPN 是 VPN 的一种，转发时依据 VPN 信息和 IP 地址转发，而不是单纯依

据 IP 地址。

参考答案

（44）A （45）B

试题（46）

很多通信使用对称密钥加密方法，其中共享密钥的分发过程是保证安全的重要环节之一，可用于在用户甲和乙之间分发共享密钥的方案是（46）。

（46）A. 甲选取密钥并通过邮件方式告诉乙
B. 甲选取密钥并通过电话告诉乙
C. 甲选取密钥后通过双方事先已有的共享密钥加密后通过网络传送给乙
D. 第三方选取密钥后通过网络传送给甲、乙

试题（46）分析

本题考查密钥管理方面的基本知识。

密钥的传送是信息安全的重要环节，显然上述 A、B、D 方案都不能较好地保证密钥的安全。

参考答案

（46）C

试题（47）

甲利用对称密钥签名体制将签过名的文件发送给乙，甲不能抵赖、乙也不能伪造签名的原因是（47）。

（47）A. 只有甲知道他的签名密钥（除可信的仲裁者外），仲裁者转发甲的签名文件给乙时附加了唯一的声明信息
B. 只有甲和乙知道共享密钥
C. 只有仲裁者同时知道所有的密钥
D. 只有乙知道甲的密钥

试题（47）分析

本题考查数字签名方面的基本知识。

典型的数字签名算法是 RSA，这是一种非对称的算法。基于私钥只有自己知道这一基本假设和密钥不可推算这一数学假设，认为签名者不能否认（抵赖）和伪造。除了这一主流方法外，也可以使用对称密钥方法实现数字签名，其方法是：A 和 B 之间签名需要一个可信任的仲裁者 C，A 和 C 之间使用对称密钥 K_A，C 和 B 之间使用对称密钥 K_B。其签名过程是：A 用 KA 加密信息并发送给 C；C 利用 KA 解密得到明文，再利用 KB 对明文和自己的证书（证明该信息是 A 发送的）加密发送给 B；B 利用 KB 解密得到明文和 C 发给的证书。

由于 C 是可信任的，因此 A、B 都不能抵赖和伪造。

参考答案

（47）A

试题（48）

RSA 是一种具有代表性的公钥加密方法，如果选定了用于加解密的两个素数分别为 37、53，则每个分组的位数是（48）。

（48）A. 10　　B. 12　　C. 18　　D. 25

试题（48）分析

本题考查加密算法方面的基本知识。

RSA 是一种分组密码算法，以分组（即数据块，不是指网络层的分组）为单位进行加解密，每一个分组看成一个数据，其值小于 n，即必须小于等于 $\log_2(n)$位。在实际应用中，分组的大小是 k 位，其中 $2^k < n \leqslant 2^{k+1}$。$n=pq$，$p$、$q$ 是两个素数，由 p、q 计算 n 很容易，但由 n 计算 p、q 却很难。此题中，$p=37$，$q=53$，$n=pq=1961$。因为 $2^{10}<1961\leqslant 2^{11}$，所以每个分组的位数为 10 位。

参考答案

（48）A

试题（49）

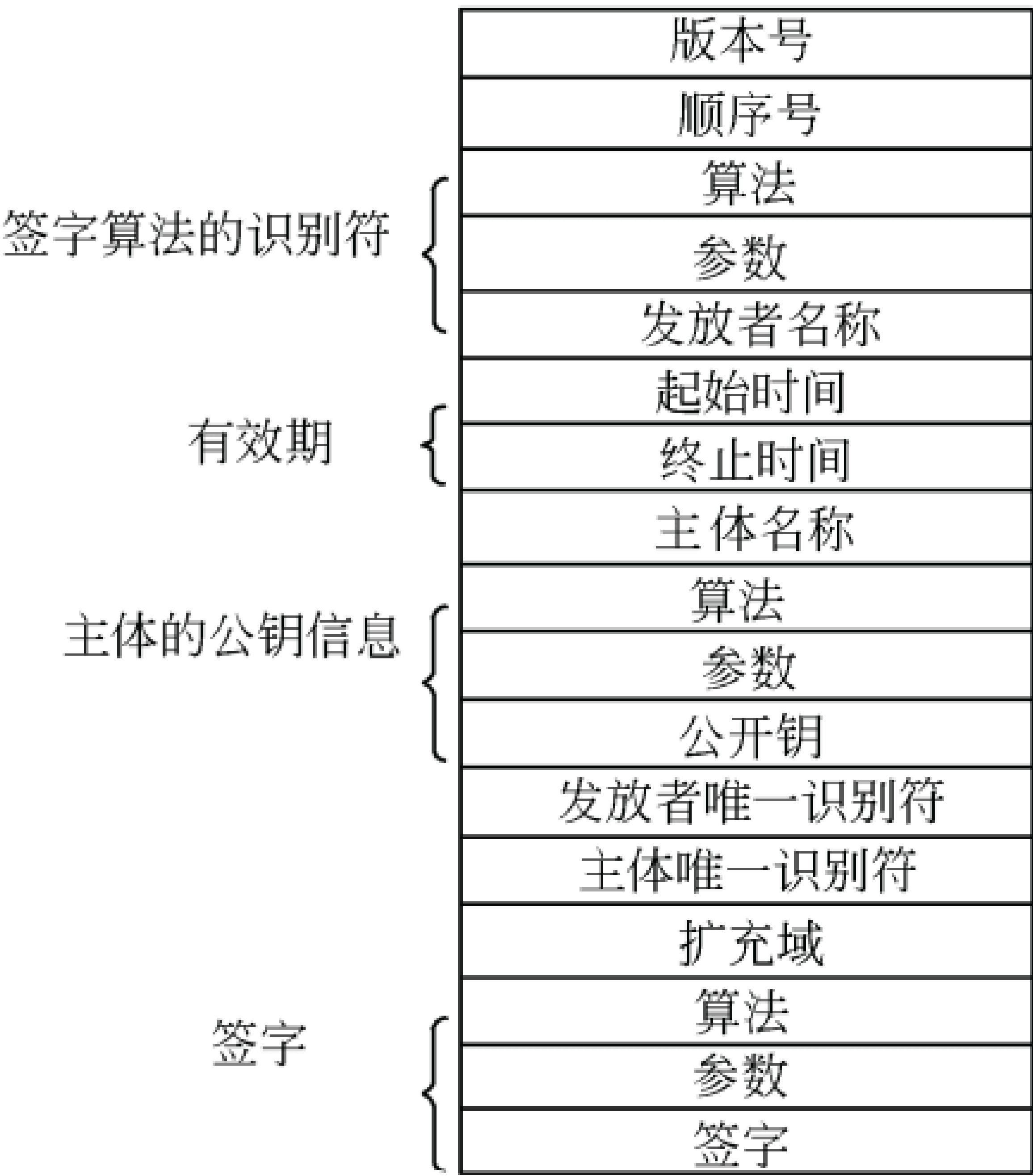
数字证书中不包含的信息是（49）。

（49）A. 公钥　　B. 私钥　　C. 起始时间　　D. 终止时间

试题（49）分析

本题考查 PKI 及数字证书的基本知识。

X.509 规定的数字证书的格式如下图所示。私钥应通过其他途径告知用户，而不应放在证书中。



参考答案

（49）B

试题（50）、（51）

针对用户的需求，设计师提出了用物理隔离来实现网络安全的方案。经过比较，决定采用隔离网闸实现物理隔离。物理隔离的思想是（50），隔离网闸的主要实现技术不包括（51）。

（50）A. 内外网隔开，不能交换信息

B. 内外网隔开，但分时与另一设备建立连接，间接实现信息交换

C. 内外网隔开，但分时对一存储设备写和读，间接实现信息交换

D. 内外网隔开，但只有在经过网管人员或网管系统认可时才能连接

（51）A. 实时开关技术　　B. 单向连接技术

C. 网络开关技术　　D. 隔离卡技术

试题（50）、（51）分析

本题考查网络安全隔离方面的基本知识。

隔离网闸的原理是基于“代理+摆渡”的概念。摆渡的思想是内外网隔开分时对网闸中的存储设备写和读，间接实现信息交换，内外网之间不能建立网络连接，以保证内外网不能通过网络协议互相访问。网闸的代理功能是数据的“拆卸”，把数据还原成原始的部分，拆除各种通信协议添加的“包头包尾”，在内外网之间传递净数据。

网闸的主要实现技术包括实时开关技术、单向连接技术和网络开关技术。

实时开关的原理是使用硬件连接两个网络，两个网络之间通过硬件开关来保证不同时连通。通过开关的快速切换，并剥去 TCP 报头，通过不可路由的数据转存池来实现数据转发。

单向连接是指数据只能从一个网络单向向另外一个网络摆渡数据，两个网络是完全断开的。单向连接实际上通过硬件实现一条“只读”的单向传输通道来保证安全隔离。

网络开关技术是将一台机器虚拟成两套设备，通过开关来确保两套设备不连通，同一时刻最多只有一个虚拟机是激活的。

参考答案

（50）C　　（51）D

试题（52）、（53）

某机构要新建一个网络，除内部办公、员工邮件等功能外，还要对外提供访问本机构网站（包括动态网页）和 FTP 服务，设计师在设计网络安全策略时，给出的方案是：利用 DMZ 保护内网不受攻击，在 DMZ 和内网之间配一个内部防火墙，在 DMZ 和 Internet 间，较好的策略是（52），在 DMZ 中最可能部署的是（53）。

（52）A. 配置一个外部防火墙，其规则为除非允许，都被禁止

B. 配置一个外部防火墙，其规则为除非禁止，都被允许

C. 不配置防火墙，自由访问，但在主机上安装杀病毒软件

D. 不配置防火墙，只在路由器上设置禁止 PING 操作

（53）A. Web 服务器，FTP 服务器，邮件服务器，相关数据库服务器

B. FTP 服务器，邮件服务器

C. Web 服务器，FTP 服务器

D. FTP 服务器，相关数据库服务器

试题（52）、（53）分析

本题考查 DMZ 和防火墙应用方面的基本知识。

DMZ 俗称非军事区，其基本思想是将内网的一些服务器另外配置一套提供给 Internet 用户访问，内网服务器不对 Internet 用户开放。这样，即使 DMZ 中的服务被攻击或被破坏，也可通过内网的原始服务器快速恢复和重建。

通常，只要 Internet 需要访问的服务都在 DMZ 中部署，包括所需要的数据库服务器。

为保证安全，在 DMZ 与内网之间部署内部防火墙，实行严格的访问限制；在 DMZ 与外网之间部署外部防火墙，施加较少的访问限制。

参考答案

（52）B　　（53）A

试题（54）～（56）

网管人员在监测网络运行状态时，发现下列现象：服务器上有大量的 TCP 连接，收到了大量源地址各异、用途不明的数据包；服务器收到大量的 ARP 报文。网管人员的判断是__（54）__，针对前一现象将采取的措施是__（55）__，针对后一现象可能采取的措施是__（56）__。

（54）A. 受到了 DoS 攻击和 ARP 攻击

B. 受到了 DDoS 攻击和 ARP 欺骗攻击

C. 受到了漏洞攻击和 DNS 欺骗攻击

D. 受到了 DDoS 攻击和 DNS 欺骗攻击

（55）A. 暂时关闭服务器

B. 暂时关闭出口路由器

C. 修改防火墙配置过滤不明数据包

D. 修改 IDS 配置使其保护服务器不受攻击

（56）A. 升级交换机内的软件

B. 加装一个内部路由器

C. 在服务器上安装 ARP 防火墙

D. 在内部网的每台主机上安装 ARP 防火墙

试题（54）～（56）分析

本题考查网络攻击与预防方面的基本知识。

DDoS 攻击的特点是收到大量源地址各异、用途不明的数据包，导致计算机耗尽 TCP 连接数或 CPU 有效时间或网络带宽等，导致不能响应正常的请求。

ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，同时使得被攻击者将信息错误地发送到伪造的地址，造成网络中断或中间人攻击。攻击者只要持续不断地发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP 地址-MAC 地址对应关系，造成网络持续不能正常工作。ARP 攻击主要是存在于局域网中，局域网中若有一台计算机感染 ARP 病毒，则感染该 ARP 病毒的系统将会试图通过“ARP 欺骗”手段截获所在网络内其他计算机的通信信息，并因此造成网内其他计算机的通信故障。解决方法是在每台计算机上安装 ARP 防火墙或杀毒软件，发现并杀掉该病毒。

参考答案

（54）B （55）C （56）D

试题（57）

下列选项中属于项目计划约束条件的是（57）。

（57）A. 过去业绩的纪录
B. 类似项目的财务报告
C. 事先确定的预算
D. 以前项目的经验

试题（57）分析

本题考查网络项目计划管理方面的基本知识。

项目计划约束是指对本项目的实施具有约束性的条件，包括预算约束、工期约束、施工条件约束、质量约束和应用产品约束等，通常是建设单位的约束条件。过去的业绩、其他项目的财务报告、以前项目的经验是承建单位的资质性条件，对完成本项目具有参考作用，但不是本项目的约束条件。

参考答案

（57）C

试题（58）

在项目进度管理中，常用（58）来安排工作顺序。

（58）A. 进度曲线法 B. 网络图法 C. 直方图法 D. 相关图法

试题（58）分析

本题考查网络项目进度管理方面的基本知识。

网络图法是一种编制大型工程进度计划的有效方法。其基本思想是将项目内容分解为工作、事件等，在一个有向图上用节点表示，用有向弧表示工作或事件之间的关联关系或时序关系（权值表示所需时间）。利用网络图，容易计算出关键路径（即项目所需的

总时间），通过改进网络、缩短关键路径的长度可以缩短项目的工期。

进度曲线法是以时间为横轴、以完成累计工作量（该工作量的具体表示内容可以是实物工程量的大小、工时消耗或费用支出额，也可以用相应的百分比来表示）为纵轴，按计划时间累计完成任务量的曲线作为预定的进度计划。进度曲线大体呈 S 形。

直方图又称质量分布图，是一种几何形图表，它是根据从生产过程中收集来的质量数据分布情况，画成以组距为底边、以频数为高度的一系列连接起来的直方型矩形图，是研究工序质量分布常用的一种统计工具。

相关图又称散布图，是在质量控制中用来显示两种质量数据之间关系的一种图形。

参考答案

（58）B

试题（59）

项目质量控制的目的是__（59）__。

（59）A. 增强满足质量要求的能力
B. 致力于提供质量要求得到满意的信任
C. 致力于满足质量要求
D. 制定质量目标、规定过程和资源，以实现其目的

试题（59）分析

本题考查项目质量管理方面的基本知识。

质量管理的目的就是采取一切必要措施并执行，以满足质量的要求。

参考答案

（59）C

试题（60）

在项目的每一个阶段结束时，审查项目完成情况与可交付成果是为了__（60）__。

（60）A. 根据项目基线确定完成项目所需的资源数量
B. 根据已完成的工作量调整时间安排与成本基线
C. 决定项目是否应进入下一阶段
D. 接受客户对所交付项目的验收

试题（60）分析

本题考查项目阶段性管理的基本知识。

在项目的每个阶段结束时，都要对项目完成情况与可交付成果进行审查，以确定项目是否应进入下一阶段。每个阶段的成果可看成是一个里程碑。

参考答案

（60）C

试题（61）

项目风险管理的工作流程是__（61）__。

（61）A. 风险辨识、风险分析、风险控制、风险转移
B. 风险辨识、风险分析、风险转移、风险控制
C. 风险辨识、风险转移、风险分析、风险控制
D. 风险转移、风险辨识、风险分析、风险控制

试题（61）分析

本题考查项目风险管理方面的基本知识。

项目风险管理有较多工作内容，其中的主要内容是风险辨识、风险分析、风险控制和风险转移，并且是按照这样的顺序一个一个地完成。容易看出，前一项工作是后一项工作的基础和条件，后一项工作是前一项工作的目的和结果。

参考答案

（61）A

试题（62）

以下不属于风险识别工作的是（62）。

（62）A. 确定风险来源　　B. 确定风险条件
C. 描述风险特征　　D. 制定风险对策

试题（62）分析

本题考查项目风险管理方面的基本知识。

风险的识别是指弄清风险的来源、风险发生的条件、风险的特征和表现。风险对策属于风险控制的范畴。

参考答案

（62）D

试题（63）

我国法律规定，计算机软件著作权的权利自软件开发完成之日起产生，对公民著作权的保护期限是（63）。

（63）A. 作者有生之年加死后 50 年　　B. 作品完成后 50 年
C. 没有限制　　D. 作者有生之年

试题（63）分析

本题考查知识产权保护方面的基本知识。

根据《中华人民共和国著作权法》和《计算机软件保护条例》的规定，计算机软件著作权的权利自软件开发完成之日起产生，公民的软件著作权保护期为公民终生及其死亡之后 50 年；法人或其他组织的软件著作权保护期为 50 年。保护期满，除开发者身份权以外，其他权利终止。一旦计算机软件著作权超出保护期后，软件进入公有领域。计算机软件著作权人的单位终止和计算机软件著作权人的公民死亡均无合法继承人的，除开发者身份权以外，该软件的其他权利进入公有领域。软件进入公有领域后成为社会公共财富，公众可无偿使用。

参考答案

（63）A

试题（64）

我国著作权法中，著作权与下列哪一项系同一概念（64）。

（64）A. 署名权　　B. 出版权　　C. 版权　　D. 专有权

试题（64）分析

本题考查著作权的基本概念。

著作权也称为版权，是指作者对其创作的作品享有的人身权和财产权。人身权包括发表权、署名权、修改权和保护作品完整权等。财产权包括作品的使用权和获得报酬权，即以复制、表演、播放、展览、发行、摄制电影、电视、录像或者改编、翻译、注释、编辑等方式使用作品的权利，以及许可他人以上述方式使用作品并由此获得报酬的权利。著作权保护的对象包括文学、科学和艺术领域内的一切作品，不论其表现形式或方式如何，诸如书籍、小册子和其他著作；讲课、演讲和其他同类性质作品；戏剧或音乐作品；舞蹈艺术作品和哑剧作品；配词或未配词的乐曲；电影作品以及与使用电影摄影艺术类似的方法表现的作品；图画、油画、建筑、雕塑、雕刻和版画；摄影作品以及使用与摄影艺术类似的方法表现的作品；与地理、地形建筑或科学技术有关的示意图、地图、设计图和草图等。

参考答案

（64）C

试题（65）

项目成本控制是指（65）。

（65）A. 对成本费用的趋势及可能达到的水平所作的分析和推断

B. 预先规定计划期内项目施工的耗费和成本要达到的水平

C. 确定各个成本项目内比预计要达到的降低额和降低率

D. 在项目施工成本的形成过程中，对形成成本的要素进行监督、调节和控制

试题（65）分析

本题考查成本控制的基本概念。

参考答案

（65）D

试题（66）

假设企业按 12%的年利率取得贷款 200000 元，要求在 5 年内每年末等额偿还，每年的偿付额应为（66）元。

（66）A. 40000　　B. 52000　　C. 55482　　D. 64000

试题（66）分析

本题考查成本控制方面的基本知识。

等额本息还款条件下，每期还款额 x 的计算公式是 $x=a\times r\times(1+r)^n/[(1+r)^n-1]$，其中 a 为贷款总额（本题为 200 000），r 为利率（本题为 0.12），n 为带宽期限（本题为 5）。

参考答案

（66）C

试题（67）

利用 M/M/1 排队论理论对分组交换和报文交换的平均延迟时间进行分析，其结果是<u>（67）</u>。

（67）A. 分组交换的平均延迟时间比报文交换的平均延时时间小

B. 分组交换的平均延迟时间比报文交换的平均延时时间大

C. 分组交换的平均延迟时间与报文交换的平均延时时间一样大

D. 要视网络的状态而定

试题（67）分析

本题考查应用数学的基本知识。

设网络的通信量强度为 ρ，报文（分组）的平均长度为 $1/\mu$，根据 M/M/1 排队论模型可知，报文交换和分组交换的平均延迟时间分别为

$T_m=2/(2\mu\times(1-\rho))$， $T_p=(2-\rho)/(2\mu\times(1-\rho))$

因为 $\rho>0$， 所以 $T_p<T_m$。

参考答案

（67）A

试题（68）

在采用 CSMA/CD 控制方式的总线网络上，设有 N 个节点，每个节点发送帧的概率为 p，则某个指定节点发送成功的概率为<u>（68）</u>。

（68）A. p B. $(1-p)^{N-1}$ C. $p(1-p)^{N-1}$ D. $Np(1-p)^{N-1}$

试题（68）分析

本题考查应用数学的基本知识及在网络中的应用。

某个节点（特指）发送成功的条件是其他 $N-1$ 个节点都没有发送，且本节点发送成功。前者的概率为$(1-p)^{N-1}$，后者的概率为 p。

参考答案

（68）C

试题（69）

某厂需要购买生产设备生产某种产品，可以选择购买四种生产能力不同的设备，市场对该产品的需求状况有三种（需求量较大、需求量中等、需求量较小）。厂方估计四种设备在各种需求状况下的收益由下页表给出，根据收益期望值最大的原则，应该购买<u>（69）</u>。

收益 设备 / 需求状况概率	设备 1	设备 2	设备 3	设备 4
需求量较大概率为 0.3	50	30	25	10
需求量中等概率为 0.4	20	25	30	10
需求量较小概率为 0.3	–20	–10	–5	10

（69）A. 设备 1　　B. 设备 2　　C. 设备 3　　D. 设备 4

试题（69）分析

本题考查运筹学方法及其应用的基本知识。

对每种设备，其收益期望值=Σ需求概率 i×预期收益 i。

据此计算得到 4 种设备的收益期望值分别为 17、16、18、10。

参考答案

（69）C

试题（70）

某公司新建一座 200 平方米的厂房，现准备布置生产某产品的设备。该公司现空闲生产该产品的甲、乙、丙、丁 4 种型号的设备各 3 台，每种型号设备每天的生产能力由下表给出，在厂房大小限定的情况下，该厂房每天最多能生产该产品（70）个。

	甲	乙	丙	丁
占地面积（平方米）	40	20	10	5
每天生产能力（个）	100	60	20	8

（70）A. 500　　B. 520　　C. 524　　D. 530

试题（70）分析

本题考查线性规划方法及其应用的基本知识。

这是一个整数背包问题。其中一种解法是贪婪法，按设备单位面积的生产能力从高到低排序，依次选取对应设备，直到把厂房面积用完。

4 种设备的单位面积生产能力分别为 2.5、3、2、1.6，所以依次选乙设备 3 台（占地 60 平方米）、甲设备 3 台（占地 120 平方米）、丙设备 2 台（占地 20 平方米），生产能力为 520。

参考答案

（70）B

试题（71）～（75）

The network layer provides services to the transport layer. It can be based on either （71）. In both cases，its main job is （72） packets from the source to the destination.

In network layer，subnets can easily become congested，increasing the delay and （73）

for packets. Network designers attempt to avoid congestion by proper design. Techniques include __(74)__ policy，caching，flow control，and more.

The next step beyond just dealing with congestion is to actually try to achieve a promised quality of service. The methods that can be used for this include buffering at the client，traffic shaping，resource __(75)__，and admission control. Approaches that have been designed for good quality of service include integrated services (including RSVP)，differentiated services，and MPLS.

（71）A. virtual circuits or datagrams　　B. TCP or UDP
　　C. TCP or IP　　D. IP or ARP
（72）A. dealing with　　B. routing
　　C. sending　　D. receiving
（73）A. lowering the throughput　　B. lowering the correctness
　　C. lowering the effectiveness　　D. lowering the preciseness
（74）A. abandonment　　B. retransmission
　　C. checksum　　D. synchronism
（75）A. distribution　　B. guarantee
　　C. scheme　　D. reservation

参考译文

网络层为传输层提供服务，它基于虚电路或数据报方式，其主要工作是对源节点的包进行路由选择，转发到目的节点。

在网络层，通信子网很容易出现拥塞，导致包的延迟增加、吞吐率降低。网络设计者试图通过良好的设计避免拥塞，所使用的技术包括重传策略、缓冲策略和流控制等。

仅仅处理拥塞是不够的，下一步的目标是试图达到设定的服务质量。可以使用的方法有客户端缓存、通信量整形、资源预留和接纳控制等。已提出的、较好的服务质量控制方法有集成服务（包括 RSVP)、区分服务和 MPLS。

参考答案

（71）A　（72）B　（73）A　（74）B　（75）D

第 2 章　2009 下半年网络规划设计师下午试卷 I 试题分析与解答

试题一（共 25 分）

阅读以下关于某城市公交集团企业网络设计的叙述，回答问题 1、问题 2 和问题 3。

某城市公交集团营运公司根据城市发展的需要，制定了公交集团 2006 年至 2010 年的信息规划。在规划中明确提出在集团范围内建设一个用于公交车辆监控、调度的企业网络，利用先进的信息化技术改造传统的管理和运作模式，大力提升公共交通的服务水平和提高运行效率、降低运行成本。

公交集团营运公司是一家拥有四个二级分公司、1 万多名职工、2000 名办公人员的国有独资公司，目前拥有公交场站 50 个、公交营运线路 250 条，日营运车辆 5000 辆，平均运距为 6 公里，线路总长度 4000 公里，每年营运的载客人数为 1 亿人次，年营运收入 130 亿元。

公交集团企业网络覆盖集团总部与四个二级分公司，要求在五年内能够对所有公交车辆完成实时轨迹监控和调度，同时能够为公交集团内部信息系统的运行提供网络支撑环境。

【问题 1】

在需求分析阶段，设计单位了解到公交集团办公人员的工作时间是早上 8:00 至下午 6:00，公交线路的运营时间是早上 5:00 至晚上 10:00，在非工作时间，监控和调度网络基本处于闲置状态。

公交集团企业网络的应用主要包括四类，分别是车辆监控调度、办公和集团营运业务、场站视频监控和互联网访问。各类应用的当前需求调查情况如表 1 所示。

表 1　公交集团应用需求调查

应用名称	产生数据情况	用户情况	应用方式	备注
车辆监控调度	所有车辆每 10 秒钟发送一次车辆的位置信息，每次信息量约 0.00007 MByte，调度指令根据需要发送，可以忽略不计	高峰期除少量车辆检修外，基本上所有车辆都要纳入监控	监控数据从移动公司传递至公交集团	预计五年后车辆增长 20%
办公和集团营运业务	平均每个办公人员每 10 分钟左右将完成两次办公或者业务操作，每次产生的数据量大致在 0.5Mbyte	上班高峰时间，所有办公人员都处于在线状态	信息中心倾向于对办公和营运业务采用 B/S 模式，即位于本部和分公司的办公人员在线访问位于集团本部的服务器	预计五年后业务的增长量为 200%

（续表）

应用名称	产生数据情况	用户情况	应用方式	备注
场站视频监控	各场站的摄像机采用 D1 格式实时采集视频流，平均每秒钟产生 0.2Mbyte 的视频码流	每个场站的大门、调度点、停车位都设置摄像头，平均每个场站5个摄像头	视频流在场站本地实时调阅，部分视频上传至集团，符合80/20规则	预计五年后业务的增长量为100%
互联网访问	办公人员可以访问互联网络，平均每个工作人员10分钟内进行2次互联网操作，每次产生的数据量约0.6MByte	信息中心希望对互联网访问进行限制，同时在线人数不超过200人	各办公人员通过集团至运营商的线路访问互联网，多为B/S类应用	预计五年后业务增长量为300%

（a）如不考虑场站视频监控系统的工作时间，请计算出公交集团监控和调度网络的可用性指标。

（b）请根据应用需求调查情况，结合五年后的增长率，计算并填写表2的内容。

表2　应用分析

应用名称	平均事务量大小（MB）	峰值用户数（个）	平均会话长度（秒）	每会话事务数（个）	增长率	五年后应用总流量（Mbps）
车辆监控调度						
办公和集团营运业务						
场站视频监控						
互联网访问						

（注：应用总流量是指由该应用在整个网络上产生的流量，本题不考虑网络数据包封装所增加的网络流量）

【问题2】

设计人员通过需求分析，认为公交集团企业网络主要由三级局域网络互连而成，这三级局域网络分别为集团总部的核心局域网、分公司局域网、场站局域网。公交集团企业网络将通过路由设备连接这些局域网，以便于承载整个集团的各类应用。

在需求分析阶段应用分析的基础上，设计人员获取了如下的信息：

- 车辆监控调度应用从移动公司网络获取车辆数据流，在集团局域网存储，分发至四个分公司，再进一步分发至各场站的监控计算机，四个分公司拥有车辆的比例为1：2：1：1；
- 办公和集团营运业务应用为B/S模式，主要由分公司、场站的办公人员发起，将形成分公司、场站之间的双向数据流，客户端至服务器占应用总流量的20%，服

务器至客户端占应用总流量的 80%，各分公司之间办公人员数量较为接近；

- 场站视频监控应用主要由场站摄像机产生视频流，符合 80/20 规则，即 80%的应用流量在本地进行实时调阅与存储，20%的流量将上传至集团局域网进行调阅和存储，四个公司之间的场站数量比例同于车辆比例；
- 互联网访问应用主要是用于分公司、场站的办公用户访问互联网，多为 B/S 类型应用访问，用户至集团局域网访问互联网的上行流量为 20%，下行流量为 80%。

基于以上资料，假设场站局域网的流量都将经过分公司局域网汇总，再传递至集团局域网，计算集团局域网至各分公司局域网的通信流量要求，填入表 3 中（通信流量要求应至少满足 5 年的应用需求）。

表 3　通信流量表

流 量 分 布	上行流量（Mbps）	下行流量（Mbps）
集团至一公司		
集团至二公司		
集团至三公司		
集团至四公司		

【问题 3】

根据公交集团的组织机构情况，设计人员形成了如图所示的逻辑网络结构。

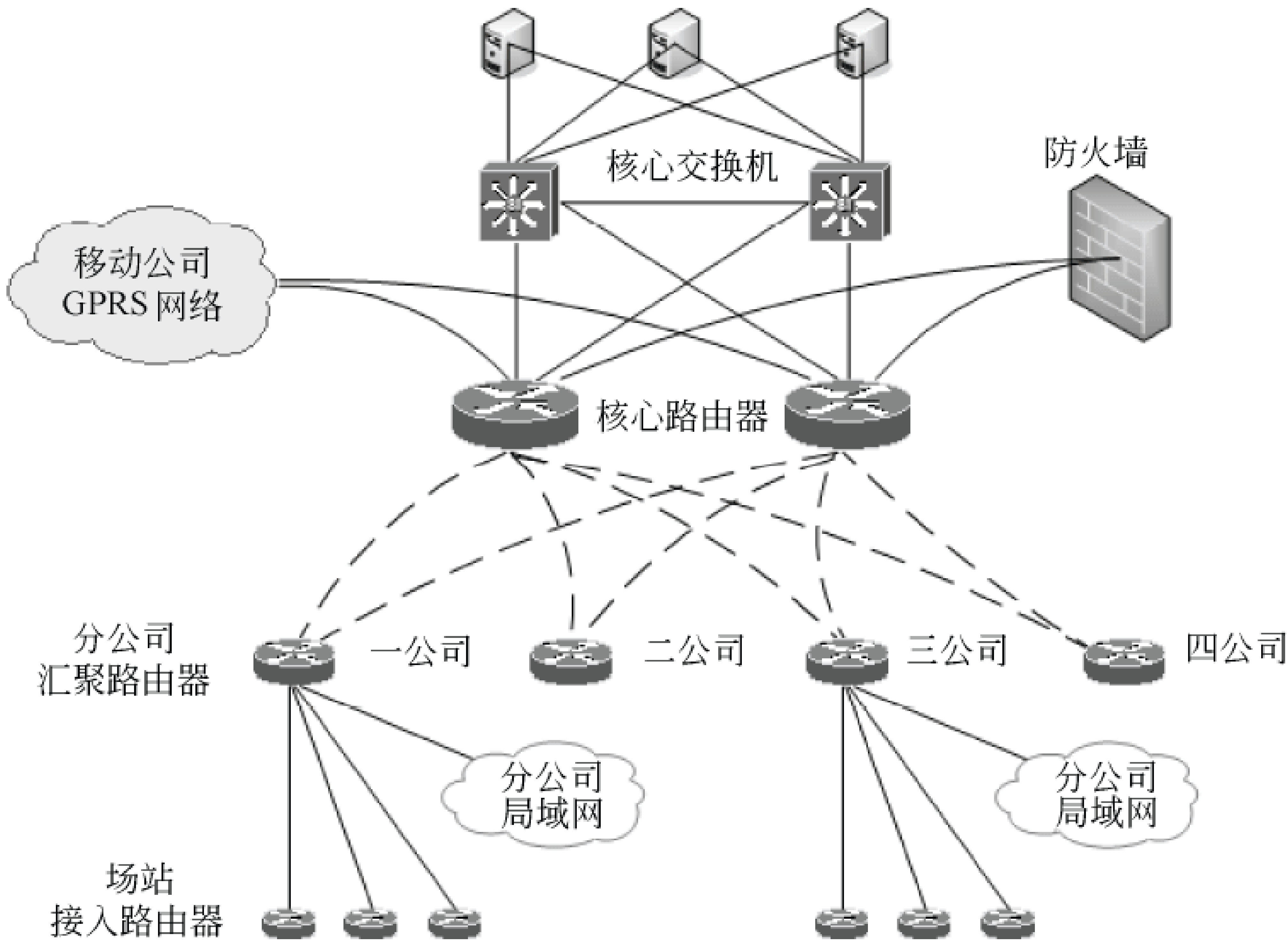


图　企业网络逻辑结构

（a）请分析该逻辑网络结构的冗余性，并指出存在的故障单点。

（b）假设网络中的所有主用线路、备用线路都是相同的线路，为了能够借助于路由

协议实现等开销路径上的负载均衡，该网络可以采用何种路由协议？

试题一分析

本题是一个典型的规划设计案例，涉及网络分析与设计过程的需求分析、逻辑网络设计、物理网络设计。

【问题 1】

（a）可用性是指网络或网络设备（如主机或服务器）可用于执行预期任务时间所占总量的百分比，通常是无故障运行时间与网络总运行时间的比值。

在实际网络工程中，可用性也用于衡量一个网络的实际使用情况，常用的计算方法是网络实际使用时间与网络总运行时间的比值。

（（12−5）+10 ）/ 24×100% ≈ 70.83%

（b）计算出应用需要传递信息的速率，可以根据公式：应用总信息传输速率＝平均事务量大小×每字节位数×每个会话事务数×平均用户数 / 平均会话长度；在实际网络工程设计中，为保证峰值情况下网络能够正常运行，可以用峰值用户数代替平均用户数进行计算；同时在考虑了增长量后，该公式修改为：应用总信息传输速率＝平均事务量大小×每字节位数×每个会话事务数×峰值用户数×（1+增长量） / 平均会话长度。

根据各类应用的需求调查情况，可以形成如下内容：

应 用 名 称	平均事务量大小（MB）	峰值用户数（个）	平均会话长度（秒）	每会话事务数（个）	增长率（%）
车辆监控调度	0.00007	5000	10	1	20
办公和集团营运业务	0.5	2000	600	2	200
场站视频监控	0.2	250	1	1	100
互联网访问	0.6	200	600	2	300

根据以上值，计算各类应用的总流量为：

车辆监控调度：0.00007×8×5000×（1+20%）/ 10 = 0.336 Mbps

办公和集团营运业务：0.5×8×2×2000×（1+200%）/ 600 = 80Mbps

场站视频监控：0.2×8×250×（1+100%）= 800Mbps

因特网访问：0.6×8×2×200×（1+300%）/600 = 12.8Mbps

【问题 2】

在通信规范分析中，最终的目标是产生通信量，其中必要的工作是分析网络中信息流量的分布问题。在整个过程中，需要依据需求分析的结果来产生单个信息流量的大小，依据通信模式、通信边界的分析，明确不同信息流在网络不同区域、边界的分布，从而获得区域、边界上总信息流量。

对于部分较为简单的网络，可以不需要进行复杂的通信流量分布分析，仅采用一些简单的方法，例如 80/20 规则、20/80 规则等。

根据题设约定的应用上下行流量分布，各应用的分析情况如下：

应用类型	上行总流量（Mbps）	下行总流量（Mbps）	公司比例
车辆监控调度	0	0.336	1:2:1:1
办公和集团营运业务	80×0.2 = 16	80×0.8 = 64	1:1:1:1
场站视频监控	800×0.2 = 160	0	1:1:1:1
因特网访问	12.8×0.2 = 2.56	12.8×0.8 = 10.24	1:1:1:1

再根据各分公司的流量比例，计算出集团局域网和各分公司局域网之间的流量分布情况如下。

（1）车辆监控调度：

总部至一、三、四公司下行：0.336/5 = 0.0672 Mbps

总部至二公司下行：0.336×2 /5 = 0.1344 Mbps

（2）办公和集团营运业务：

总部至各分公司下行：80×0.8 /4 = 16 Mbps

各分公司至总部上行：80×0.2 /4 = 4 Mbps

（3）场站视频监控：

总部至一、三、四公司上行：800×0.2 /5 = 32 Mbps

总部至二公司上行：800×0.2×2 /5 = 64 Mbps

（4）因特网访问：

总部至各分公司下行：12.8×0.8 /4 = 2.56 Mbps

各分公司至总部上行：12.8×0.2 /4 = 0.64 Mbps

（5）流量计算：

一公司上行：4+32+0.64 = 36.64 Mbps

一公司下行：0.0672+16+2.56 = 18.6272 Mbps

二公司上行：4+64+0.64 = 68.64 Mbps

二公司下行：0.1344+16+2.56 = 18.6944 Mbps

三、四公司与一公司流量相同。

【问题 3】

（a）冗余度是另一个在网络设备和系统设计与实施中需要考虑的因素，主要通过在网络设计中通过增加冗余设备、冗余线路等方式来避免设备或线路失效对网络产生影响。随着计算机网络技术的发展，冗余度也不再仅局限于设备和线路层次，更多的冗余度开始体现到网络设备的模块、部件层次，目前在网络设计中，为关键网络设备添加冗余处理引擎、冗余电源等方式已经成为常见的技术手段。

在公交企业网络中，集团内部的核心局域网络和分公司局域网络之间通过路由器互连，每个分公司局域网络的汇聚路由器都存在两条链路和核心局域网络的核心路由器互连；两条链路都处于使用状态，无论是采用热备方式还是负载均衡方式，在任何一条链路出现故障后，分公司局域网络都能够继续完成和核心局域网络的通信。

另外，网络中存在两台核心交换机，当运行 HSRP 或者 VRRP 协议时，两台交换机工作在热备方式，甚至是互为热备方式，任何一台交换机出现故障，网络中的服务器仍

然可以对网络用户提供服务；网络中存在两台核心路由器，都参与路由运算，任何一台路由器出现故障，都会触发路由算法进行路由重新计算，从而在分公司局域网和核心局域网之间形成新的路径。因此，网络中的所有网络设备出现故障，都不会导致网络出现故障而影响应用。

该企业的逻辑网络中还存在一些缺陷，一旦发生故障，会导致网络出现一些异常：

（1）防火墙是整个公交企业网络访问因特网的关键设备，一旦该设备出现故障，就会导致整个公交企业网络与因特网断开，企业网络内的用户无法访问因特网的任何资源。

（2）各分公司的局域网络通过一台汇聚路由器连接至核心路由器，一旦分公司的汇聚路由器出现故障，就使得分公司局域网与整个企业网络断开，导致分公司用户无法访问企业网络和因特网资源。

（3）每个分公司场站的局域网通过一个接入路由器和一条链路连接至分公司的汇聚路由器，无论是接入路由器还是链路出现故障，都会导致场站局域网和企业网络断开，场站的用户将无法访问企业网和因特网资源。

（b）RIP 和 RIPv2 使用跳跃数来选择最优路径，IGRP 通过把跳跃数与带宽、延迟、可靠性和负载合成考虑，从而提高了选择最优路径的能力。

IP 不支持等开销路径上的负载均衡，但是 RIPv2 则在等开销路径上对同一个目的网或子网的报文进行负载平衡。

IGRP 对去同一目的网络或子网的报文也可以实施等代价路径的负载平衡，这种负载平衡是以时间片轮转的方式工作的。

参考答案

【问题 1】

（a）网络可用性为：（（12–5）+10 ）/ 24×100% ≈ 70.83%

（b）

应 用 名 称	平均事务量大小（MB）	峰值用户数（个）	平均会话长度（秒）	每会话事务数（个）	增长率(%)	五年后应用总流量（Mbps）
车辆监控调度	0.00007	5000	10	1	20	0.336
办公和集团营运业务	0.5	2000	600	2	200	80
场站视频监控	0.2	250	1	1	100	800
互联网访问	0.6	200	600	2	300	12.8

【问题 2】

流 量 分 布	上行流量（Mbps）	下行流量（Mbps）
集团至一公司	36.64	18.6272
集团至二公司	68.64	18.6944
集团至三公司	36.64	18.6272
集团至四公司	36.64	18.6272

【问题 3】

（a）该逻辑网络结构的冗余性分析：

- 在核心路由器和汇聚路由器之间，实现了线路的冗余；
- 网络的核心设备实现了设备冗余。

逻辑网络结构存在的故障单点：

- 防火墙是故障单点，一旦出现故障，则整个企业网络不能访问外部网络；
- 各分公司的路由器是故障单点，一旦出现故障，整个分公司无法访问企业网络；
- 分公司和场站之间的线路、场站的路由器是故障单点，一旦出现故障，场站网络将无法访问企业网络。

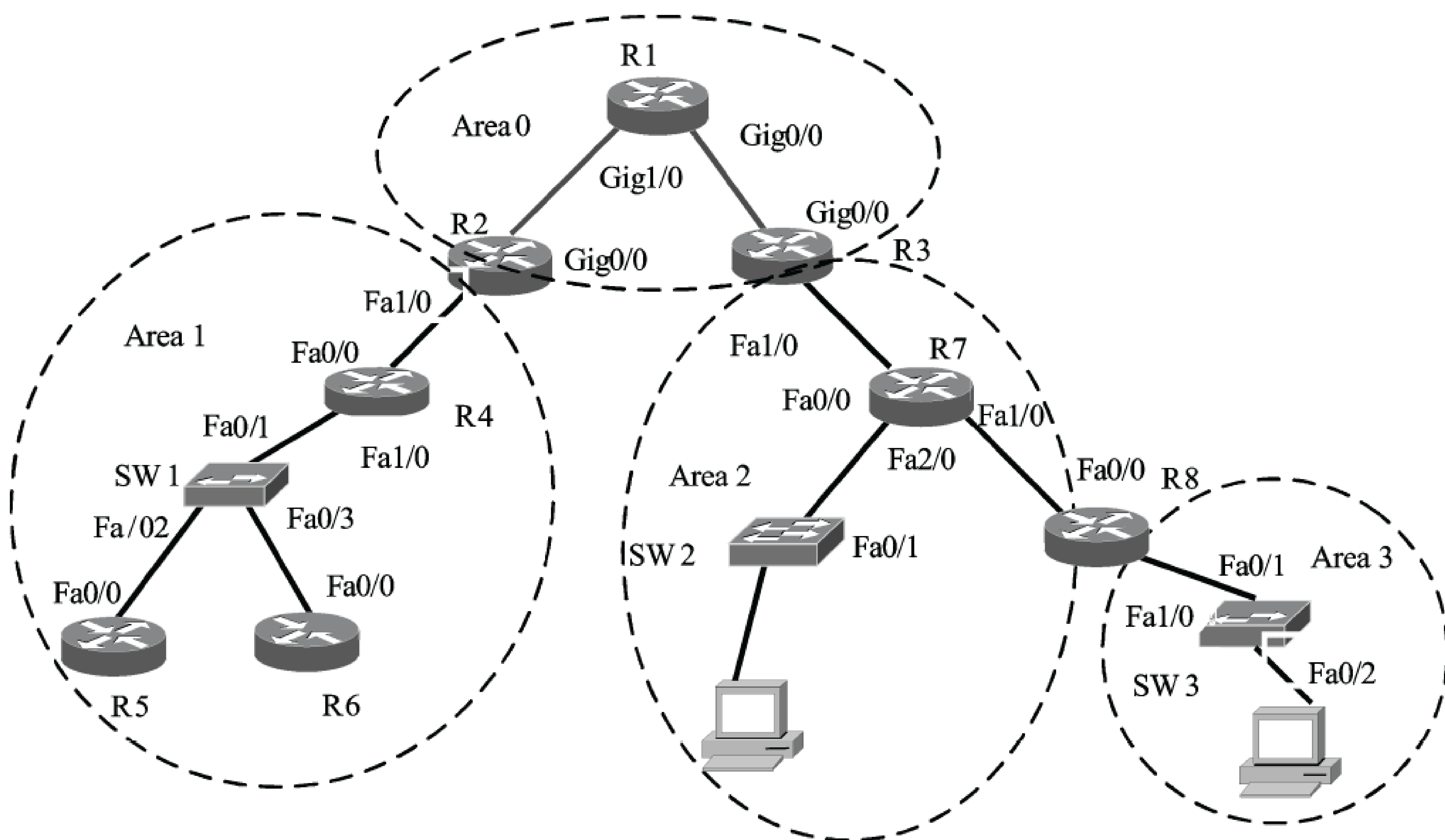
（b）RIPv2

IGRP

试题二（25 分）

阅读以下关于某网络系统结构的叙述，回答问题 1、问题 2 和问题 3。

某公司的网络结构如下图所示，所有路由器、交换机都采用 Cisco 产品，路由协议采用 OSPF 协议，路由器各接口的 IP 地址参数等如下页表所示。



网络结构

表　路由器接口信息

路由器	接口	IP 地址	子网掩码
R1	Gig0/0	10.2.0.1	255.255.255.252
	Gig1/0	10.1.0.1	255.255.255.252
	Loopback 0	192.168.0.1	255.255.255.255
R2	Gig0/0	10.1.0.2	255.255.255.252
	Fa1/0	10.9.0.1	255.255.0.0
	Loopback 0	192.168.0.2	255.255.255.255
R3	Gig0/0	10.2.0.2	255.255.255.252
	Fa1/0	10.192.0.1	255.255.255.252
	Loopback 0	192.168.0.3	255.255.255.255
R4	Fa0/0	10.9.0.2	255.255.0.0
	Fa1/0	10.8.0.1	255.255.255.0
	Loopback 0	192.168.0.4	255.255.255.255
R5	Fa0/0	10.8.0.2	255.255.255.0
	Loopback 0	192.168.0.5	255.255.255.255
R6	Fa0/0	10.8.0.3	255.255.255.0
	Loopback 0	192.168.0.6	255.255.255.255
R7	Fa0/0	10.192.0.2	255.255.255.252
	Fa1/0	10.193.0.1	255.255.0.0
	Fa2/0	10.194.0.1	255.255.0.0
	Loopback 0	192.168.0.7	255.255.255.255
R8	Fa0/0	10.193.0.2	255.255.0.0
	Fa1/0	10.224.0.1	255.255.0.0
	Loopback 0	192.168.0.8	255.255.255.255

为了保证各区域的地址连续性，便于实现路由汇总，各区域的地址范围如下：

Area 0 ——10.0.0.0/13

Area 1 ——10.8.0.0/13

Area 2 ——10.192.0.0/13

Area 3 ——10.224.0.0/13

【问题 1】

假设路由体系中 OSPF 进程号的 ID 为 1，则对于拥有三个快速以太网接口的路由器 R7，如果仅希望 OSPF 进程和接口 Fa0/0、Fa1/0 相关联，而不和 Fa2/0 关联，也就是说只允许接口 Fa0/0、Fa1/0 使用 OSPF 进程，请写出路由器 R7 上的 OSPF 进程配置。

【问题 2】

在 Area 1 中，路由器 R4、R5 和 R6 通过一台交换机构成的广播局域网络互连，各路由器 ID 由路由器的 loopback 接口地址指定，如指定 R4 是指派路由器（Designated Routers，DR）、R5 为备份的指派路由器（Backup Designated Router，BDR），而 R6 不参与指派路由器的选择过程。

配置路由器 R6 时，为使其不参与指派路由器的选择过程，需要在其接口 Fa0/0 上添加配置命令__（a）__。

在配置路由器 R4 与 R5 时，如果允许修改路由器的 loopback 接口地址，可以采用两种方式，让 R4 成为 DR，而 R5 成为 BDR，这两种可行的方法分别是：

（b）＿＿。

（c）＿＿。

【问题 3】

OSPF 协议要求所有的区域都连接到 OSPF 主干区域 0，当一个区域和 OSPF 主干区域 0 的网络之间不存在物理连接或创建物理连接代价过高时，可以通过创建 OSPF 虚链路（virtual link）的方式完成断开区域和主干区域的互连。在该公司的网络中，区域 3 和区域 0 之间也需要通过虚拟链路方式进行连接，请给出路由器 R3 和路由器 R8 上的 OSPF 进程配置信息。

试题二分析

本题是一个典型的网络配置案例，主要涉及 OSPF 路由算法的配置。

【问题 1】

关于创建 OSPF 进程，并配置进程与网络接口关联的相关命令如下。

（注：以下的命令介绍中，黑体部分是命令关键字，斜体部分是可填充的命令参数）

（1）配置命令一：　**router ospf** *process-id*。

定义 router ospf 及其后的 process-id 号，可以启动一个使用指定 process-id 的 OSPF 路由协议进程，该值并不用于标识不同的 OSPF 自治系统，而仅仅是一个进程号。通过为每个进程使用唯一的 process-id，多个 OSPF 进程能够在任何给定的路由器上执行。

（2）配置命令二：**network** *address wildcard-mask* **area** *area-id*。

定义的 OSPF 进程必须与路由器上的一个活跃 IP 接口相关联，以便 OSPF 能够开始创建邻居邻接关系和路由表。

address 参数可以是接口的 IP 地址、子网或者 OSPF 路由所用接口的网络地址；

wildcard-mask 参数为网络掩码的反码；

area-id 参数是区域号码。

当路由器接口的 IP 地址属于 address、wildcard-mask 参数所确定的子网时，该接口在活跃状态时将与 OSPF 相关联。

【问题 2】

在一个 OSPF 路由体系中，若干个路由器可能都通过各自的网络接口连接至一个广播网络中，在这个广播网络上可以预先确定 DR（指派路由器）和 BDR（备份指派路由器）。在这种方式下，OSPF 将启用精简的链路状态更新报文，LSA 只能传送到已分配的 DR 和 BDR 路由器，可以有效避免链路状态更新报文自身的广播。同时，也可以有效避免由于所有路由器都有条件作为 DR，而产生的“选举风暴”。

在产生了 DR 和 BDR 之后，一旦 DR 失效，则 BDR 会自动成为 DR。DR 选择处理过程通过发现在 OSPF 广播网络上的哪个路由器具有最高路由器优先级来实现，而由 OSPF

广播网络中的路由器提供的次高路由器优先级值为 BDR。使用接口命令 ip ospf priority 设定路由器优先级，该命令的格式如下：

```
ip ospf priority number
```

number 参数值取值范围是 0～255，其中 0 是默认值，255 是所允许的最高值。当路由器某接口的 ip ospf priority 值为 0，则表明该路由器在接口所连接的广播网络中没有条件作为 DR，从而不会参与到选择过程。在 DR 选择过程中，决定两个路由器接口优先级的规则如下：

（1）如果路由器 A 连入广播网接口的 ip ospf priority 高于路由器 B 的连入接口，则 A 优先级高于 B；

（2）如果路由器 A 和路由器 B 连入广播网接口的 ip ospf priority 值相同，则由两台路由器的 lookback 接口地址的大小来决定路由器 A 与 B 的优先级。

【问题 3】

OSPF 虚链路提供了一条从断开区域到主干区域的逻辑通路。

虚链路具有多种用途，第一种用途是连接一个没有物理连接的远程区域到主干区域，第二种用途是添加一个连接到一个断开的主干区域，第三种用途是当一个路由器失效引起主干区域分隔时提供冗余。

连接断开区域的逻辑通路必须是在这样两个路由器上定义的虚链路：这两个路由器共享公共的区域，并且其中一个路由器必须连接到主干区域。

配置虚拟链路的命令格式如下：

```
area area-id virtual-link router-id [ hello-interval seconds ] [ retrains-mit-interval seconds ] [ transmit-delay seconds ] [ dead-interval seconds ] [ authentication-key key ]
```

area-id 参数是十进制数或 IP 地址点分十进制格式的标识符，用以标识某个区域，该区域作为虚链路的转接区域，即两个路由器的共享区域；

router-id 参数是端点的路由器 ID，通常是回送接口的地址，路由器定义的虚链路到该端点；

关键字 hello-interval 的参数 seconds 默认值为 10s，指定路由器在虚链路上发送 Hello 报文之间等待的时间秒数；

关键字 retransmit-interval 的参数 seconds 默认值为 5s，该值指定重传 LSA 到邻接路由器的时间间隔，以秒为单位；

关键字 transmit-delay 的参数 seconds 默认值为 1s，该值指定 LSU 报文在传送到虚链路上之前的生存时间值；

关键字 dead-interval 的参数 seconds 默认值为 Hello 间隔的 4 倍，以秒为单位，它是在路由器没有从虚链路的远端接收到 Hello 报文的期满时间，以便声明远端路由器故障；

关键字 authentication-key 的参数 key 值是发往远端虚链路的 Hello 报文中使用的口令，用以认证远端路由器。

通常情况下，只需设置“**area** *area-id* **virtual-link** *router-id*”部分即可。

参考答案

【问题 1】

```
router  ospf  1
network  10.192.0.0  0.1.255.255  area  2
```

或者

```
router  ospf  1
    network  10.192.0.0  0.0.255.255  area  2
    network  10.193.0.0  0.0.255.255  area  2
```

【问题 2】

（a）ip　ospf　priority　0

（b）设置路由器 R4 接口 Fa1/0 的 ip　ospf　priority 值高于路由器 R5 接口 Fa0/0

（c）将路由器 R4 接口 Fa1/0 和路由器 R5 接口 Fa0/0 的 ip　ospf　priority 值设置为相等，将路由器 R4 的 loopback 接口地址设置为高于路由器 R5 的 loopback 接口地址

（注：b 和 c 答案的顺序可以互换）

【问题 3】

路由器 R3

```
router  ospf  1
area  2  virtual-link  192.168.0.8
  network  10.0.0.0  0.7.255.255  area  0
network  10.192.0.0  0.7.255.255  area  2
```

路由器 R8

```
router  ospf 1
area  2  virtual-link  192.168.0.3
  network  10.192.0.0  0.7.255.255  area  2
network  10.224.0.0  0.7.255.255  area  3
```

试题三（25 分）

阅读以下关于某公司企业广域网络升级改造的需求，回答问题 1、问题 2 和问题 3。

某高速公路沿线企业广域网主要连接公司总部和 4 个分支机构单位，为公司内部人员之间提供数据传输和业务运行环境。

网络于 2003 年建成，各网络节点之间的初始带宽为 512kbps，2005 年经设备改造后，

各节点之间带宽升级为 2Mbps，2007 年带宽进一步提升至 4Mbps。

（1）网络设备

位于公司总部的核心路由器为华为公司的 NE05，2004 年配置；通过该设备连接各分支机构的接入路由器，各接入路由器为思科公司的 2600，2003-2004 年配置；公司总部的局域网由思科公司的多层交换机 catalyst 4006 为主干设备构成，各分支机构的局域网络由华为公司 6506 三层交换机为主干设备构成。如图 1 所示。

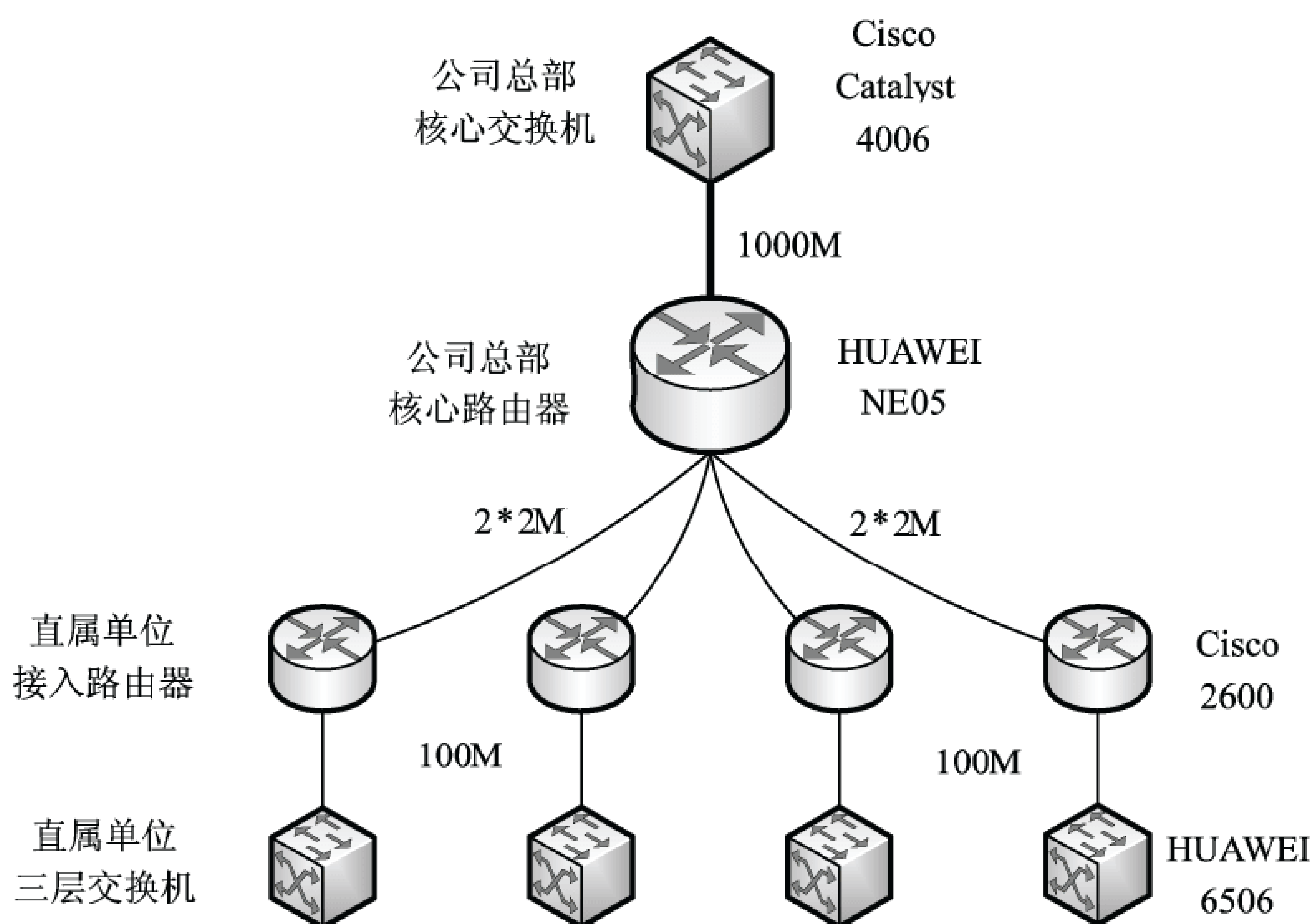


图 1 某公司广域网络设备连接

（2）网络缺陷

随着网络用户的不断增加，各种新应用、新业务的开展，对网络带宽、安全性、稳定性都提出了更高的要求。该企业广域网络存在以下问题：

- 核心至二级站点间带宽只有 4Mbps，随着高清视频会议等系统的建设，现有网络带宽已经不能满足应用需求；
- 数据设备使用年限较长，配置低，无法进行扩容，随着业务量急剧增大，将无法维持系统正常运转，也不能胜任网络升级的需要；
- 华为 NE05 型号路由器已停产，配件、模块较难购置，设备不定期会出现丢包现象，影响网络稳定；
- 路由设备均是单点结构，存在单点故障，安全性低。

（3）各类应用带宽

根据用户对企业内部现有典型应用的流量分析，考虑到各应用在两年内的正常业务增长，形成了如下表所示的典型应用带宽需求。

表　典型应用带宽需求

业务序号	应用业务	所需带宽
1	高清视频会议系统	2M～8M
2	视频监控	4M
3	IP 电话、日常办公	2M
4	业务管理类数据传送	4M
5	文本、图片、声音、图像等传输	4M
6	核心业务系统	4M
7	预留	10M

（4）升级目标

本次升级改造主要达到以下的目标：

- 对核心和分支机构路由设备进行更新，并与原有系统形成设备、链路双备份，增强安全性；
- 将核心到各个分支机构数据网络带宽进行升级；
- 根据应用业务的特性，采用 QoS 技术，确保广域网络的服务质量。

【问题 1】

现有网络主要依托高速公路沿线的 SDH 传输系统进行建设，核心路由器与各接入路由器之间的逻辑链路由若干 E1 电路组成，当前的 4M 带宽就是由两条 E1 电路绑定而形成的。

（a）已知 SDH 传输系统至公司总部的传输带宽为 STM-1，请简要分析核心路由器 NE05 上连接传输系统的传输板卡特性。

（b）如果在公司总部不增加任何设备和板卡，仅通过为每个逻辑通道绑定更多 E1 线路的方式增加带宽，则在公司总部至各分支机构带宽相等的要求下，请给出理论上公司总部至各分支机构可以扩充的最大带宽。

【问题 2】

设计单位决定为公司总部分别添加一台核心路由器和核心多层交换机，并且采用了如图 2 所示的连接方式，请简要分析该连接方式与原有方式相比较，具有哪些优势。

【问题 3】

设计单位决定将现有线路、路由设备，作为企业网络的备份线路及备份路由体系，同时在总部和分支机构添置相应的路由器，形成主用路由体系。用户单位提出了一个明确的需求，希望本次新采购的路由设备主要采用以太网口，以避免线路带宽升级时，用户端设备频繁发生变化。

升级设计方案中，要求 SDH 系统的局端传输设备完成协议转换工作，直接提供以太网接口，并互连至总部和分支结构的路由器以太网接口。假设总部至分支结构的链路是由大于 10 条以上 E1 绑定形成，请简要分析总部的核心路由器千兆以太网与传输设备千兆以太网之间可能存在的工作机制，并针对每种工作机制说明核心路由器如何区分来

自不同接入路由器的数据包。

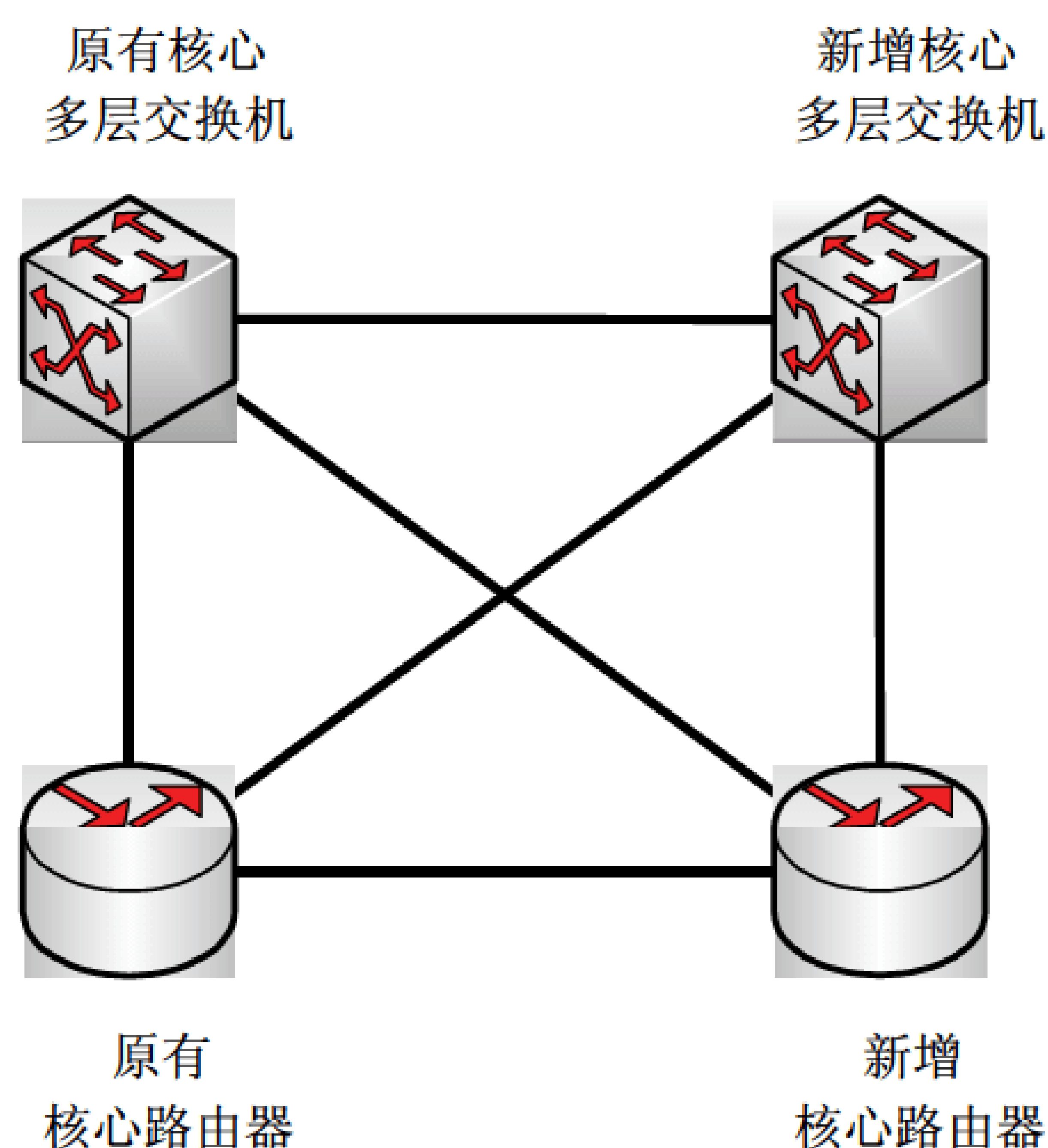


图 2　公司总部设备连接方式

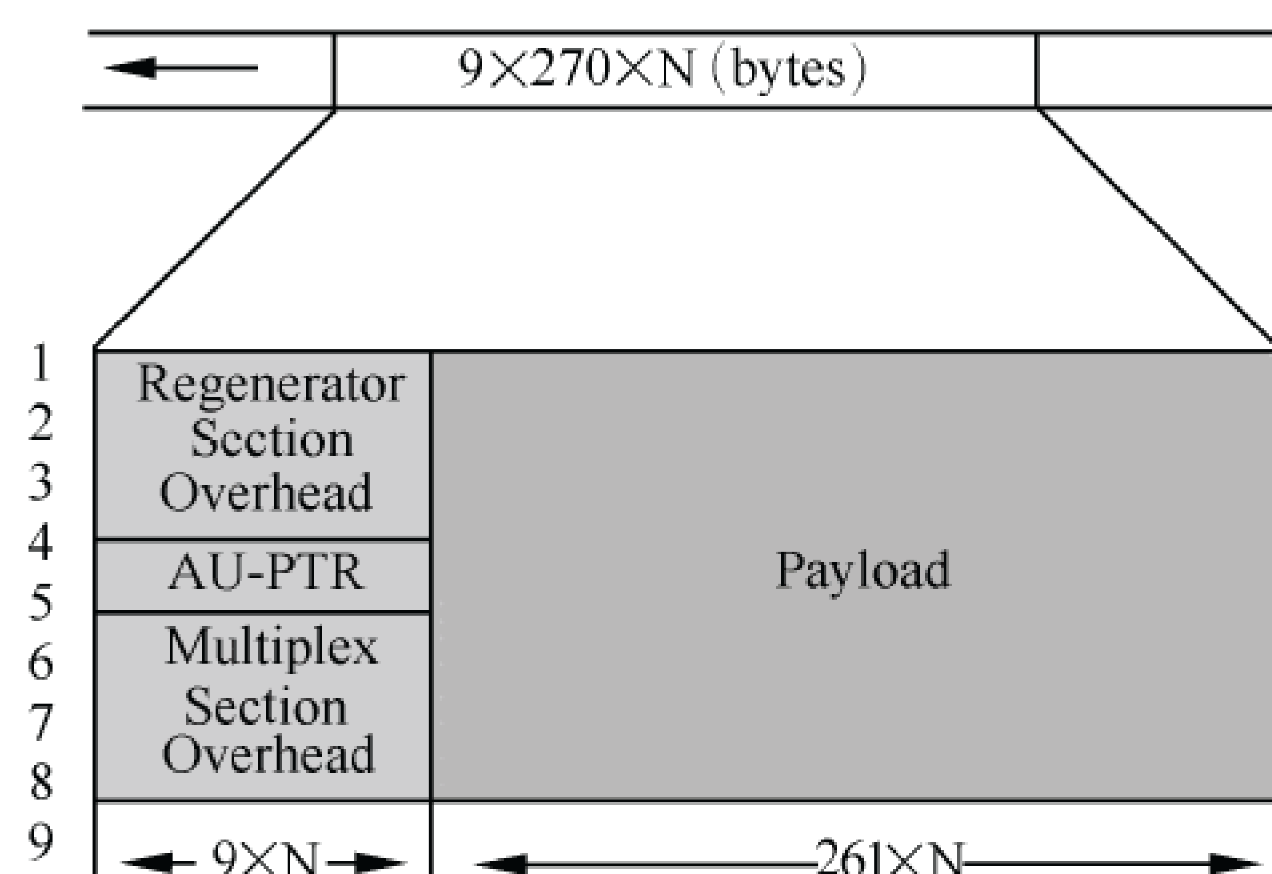
试题三分析

本题是一个典型的升级改造案例，涉及现有网络缺点分析、改造设计和设备利用等知识。

【问题 1】

SDH（Synchronous Digital Hierarchy，同步数字系列）是 CCITT（现在的 ITU-T）定义的，采用同步复用方式和灵活的映射结构，可以从 SDH 信号中直接分插出低速的支路信号，而不需要使用大量的复接/分接设备，从而能够减少信号损耗和设备投资。

为方便地从高速信号中直接分/插低速支路信号，应尽可能使低速支路信号在一帧内均匀地、有规律地分布。ITU-T 规定 STM-N 的帧采用以字节为单位的矩形块状结构，如下图所示。



STM-N 是 9 行×270×N 列的块状帧结构，此处的 N 与 STM-N 的 N 相一致，取值

范围为 1，4，16，…，表示此信号由 N 个 STM-1 信号复用而成。STM-1 帧为 9 行×270 列的结构，其中前 10 列为开销，后 260 列为净负荷，STM-1 的速率为 155.52Mbps。

由于 SDH 的最低速率 STM-1 也大于 155Mbps，无法应对用户提出的细粒度带宽需求，因此允许传统的数字载波体系——E 标准和 T 标准体系，将 SDH 体系作为传输承载层，采用同步时分复用方式，向用户提供低速带宽链路服务。

当把 SDH 信号看成由低速信号复用而成时，这些低速支路信号就称为通道。而 CPOS 是通道化 SDH/SONET 接口模块的简称，其中 C 表示 Channelized，POS 表示 Packet Over SDH/Sonet。它充分利用了 SDH 体制的特点，提供对带宽精细划分的能力，可减少组网中对路由器低速物理接口的数量要求，增强路由器的低速接口汇聚能力，并提高路由器的专线接入能力。

CPOS 接口具有如下特性：

（1）CPOS 支持 STM-1/OC-3 多通道接口模块，支持 155.52Mbps 的通信速率。

（2）CPOS 接口卡分为 CPOS（E）和 CPOS（T）两种型号，其中 CPOS（E）接口卡支持 E 标准制式，而 CPOS（T）接口卡支持 T 标准制式。

（3）CPOS 接口模块通过 PCI 接口与 CPU 进行通信，完成 STM-1 通道化 POS 接口数据的收发。

（4）STM-1 CPOS 接口支持净通道（非成帧）E1（最多 63 个）或 T1（最多 84 个）。

（5）STM-1 支持非通道化（成帧）E1（最多 63 个）或 T1（最多 84 个）。

（6）STM-1 支持通道化到 64K，但是最多 256 个逻辑通道。

在目前的实现中，CPOS 接口多实现 E1、T1 向 STM-1 的复用，我国 SDH 体制选用的是 E1、T1 向 STM-1 的复用；CPOS 通道化 E1 支持净通道（clear channel，又称为非成帧模式，unframed）和非通道化（unchannelized）两种工作模式。在净通道模式下，E1 通道不分时隙，形成一个速率为 2.048Mbps 的串口（相当于一个 2.048Mbps 的同步串口）。在非通道化模式下，E1 通道除时隙 0 以外的 31 个时隙可以捆绑为一个串口使用（相当于一个 E1-F 端口）。

在骨干网的核心路由器上使用一个 155M CPOS 模块，配置为通道化至 E1，连接到 SDH 传输网，与汇聚层路由器所用的 E1 接口相连。也可根据需要对 E1 口进行捆绑，提高汇聚层设备的接入带宽。

【问题 2】

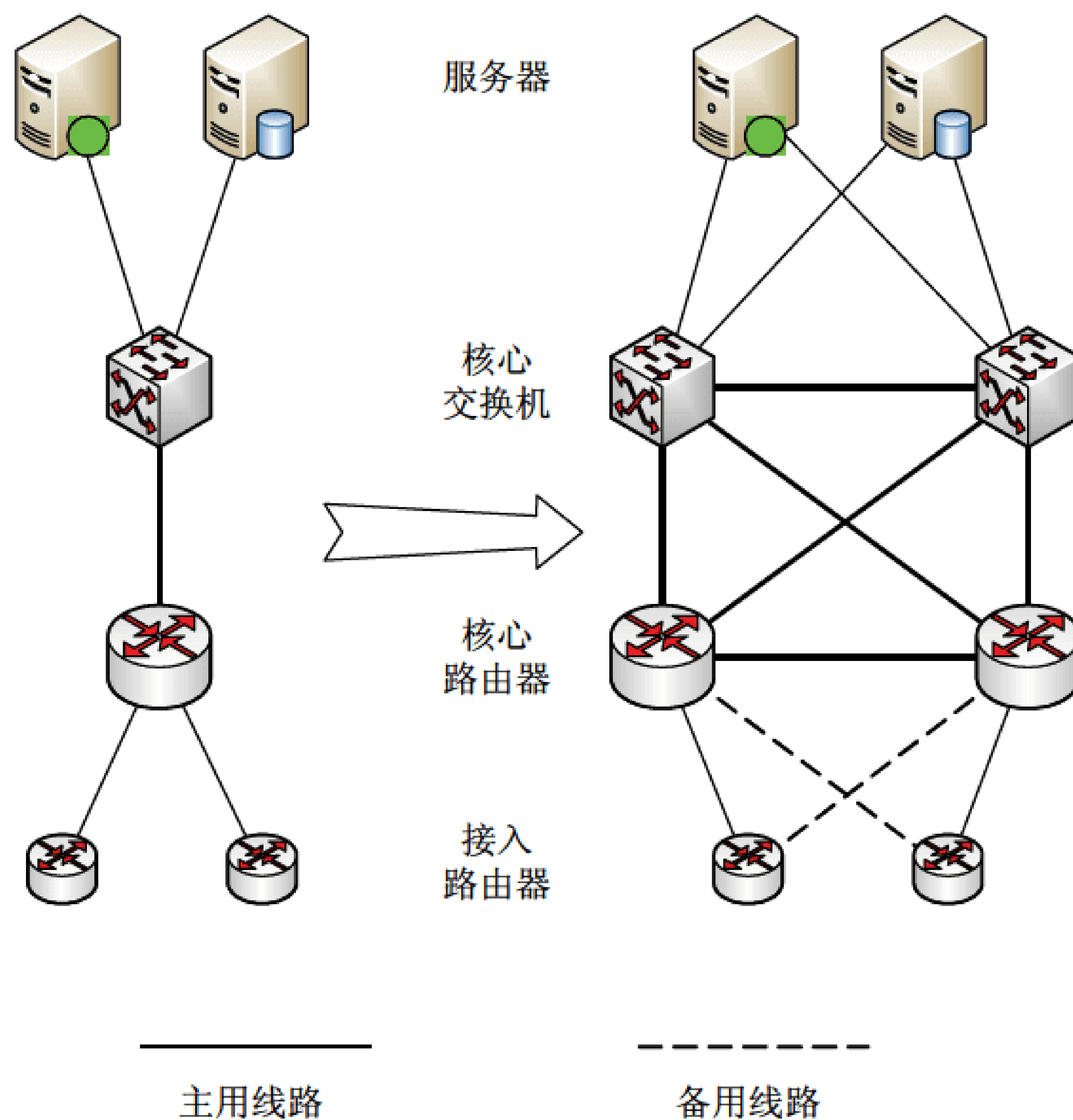
在对网络设备进行添置前后，服务器和接入路由器与核心设备的连接方式将发生改变，如下图所示。

对两种结构的分析如下：

（1）在新结构中，多层交换机、核心路由器分别存在两台，并且每台核心设备与其他核心设备都存在链路，形成了核心设备的全互联结构（Full mesh）。在当前案例中，两条以下的链路失效不会导致网络的瘫痪。

（2）当任何一台核心多层交换机失效之后，另外一台核心交换机仍可以处于工作状态，服务器的访问流量将由活跃的核心多层交换机承担；当任何一台核心路由器失效之

后，动态路由算法将修改路径信息，使得活跃的核心路由器承载下级网络访问核心局域网络的流量。因此任何一台核心设备的失效都不会导致网络瘫痪。



（3）由于网络中存在两台核心多层交换机，因此可以在这两台交换机之间加载冗余网关协议，例如 HSRP、VRRP 和 GLBP 等。当使用 HSRP、VRRP 协议时，对于局域的默认网关地址来说，一台交换机主用，一台交换机备用，可以通过为核心局域网设立两个默认网关地址方式实现两台交换机的负载均衡；当使用 GLBP 协议时，协议会自动实现交换机的负载均衡。

（4）由于网络中存在两台核心交换机，因此下级网络的接入路由器至核心路由器就存在两条链路，通常情况下一条为主用链路，一条为备用链路。如果主用链路和备用链路带宽等不相同，可以通过交叉互连方式实现核心路由器的负载均衡；如果主用链路和备用链路带宽等相同，就可以采用 RIPv2、IGRP 等路由协议实现等开销路径上的负载均衡。

【问题 3】

总部的核心路由器千兆以太口与传输设备千兆以太口之间可能存在的工作机制主要包括两种：子接口方式和 VLAN 方式，其分析详见参考答案。

参考答案

【问题 1】

（a）

- 该板卡支持 STM-1 155Mbps 的通道化 POS（Channelized POS，CPOS）接口，也就是可以对 155M 的 STM-1 进行时隙划分成若干电路；
- 电路划分的细粒度为 E1；

- 同时支持将多个 E1 电路绑定成逻辑链路。

（b）一个 STM-1 的 CPOS 接口最多可以划分为 63 个 E1 电路。由于要求公司总部和 4 个分支机构之间带宽相等，因此理论上每个逻辑链路最多由 15 个 E1 电路绑定。最大带宽为 2.048×15=30.71Mbps。

【问题 2】

具有如下优势：

（1）各路由设备之间采用全互联结构，保证任何两条链路中断，所有路由设备之间可以互访；

（2）不存在设备级的单点故障，任何设备的损坏不影响网络的运行；

（3）两台多层交换机之间可以运行 HSRP、VRRP 和 GLBP 等冗余网关协议，保证一台交换机出现故障时，服务器可以继续提供服务；

（4）借助于路由算法、策略路由等技术，可以实现网络流量的负载均衡。

【问题 3】

存在两种工作方式：

（1）子接口方式。路由器千兆以太网络接口划分成若干的逻辑子接口，传输设备将不同分支路由器的捆绑 E1 电路上的数据帧映射至不同的子接口，核心路由器通过逻辑子接口来确定数据帧的来源路由器。

（2）VLAN 方式。路由器和传输设备的千兆以太网接口都工作在 VLAN Trunk 模式下，传输设备将不同分支路由器的捆绑 E1 电路上的数据帧映射至不同的 VLAN 中，路由器千兆接口利用接收到数据帧的 VLAN 标签来决定该数据帧的来源路由器。

第3章　2009下半年网络规划设计师下午试卷II写作要点

试题一　论电子政务专用网络的规划与设计

随着信息技术在世界范围内的迅猛发展，特别是网络技术的普及应用，电子政务正在成为当代信息化的最重要领域之一。电子政务的推进加快了政府职能转变，提高了政府办事效率，增强了政府服务能力，促进了政务公开和廉政建设。电子政务的实施依托于电子政务专用网络，因而电子政务专用网络有其特有的应用环境和需求，也需要采用特有的技术和方法。

请围绕“电子政务专用网络的规划与设计”论题，依次对以下三个方面进行论述。

1. 概要叙述你参与设计和实施的电子政务专用网络项目（若没有，叙述类似的项目）以及你所担任的主要工作。

2. 具体讨论你在电子政务专用网络（或类似网络）规划与设计中针对特有的应用环境和需求采用了哪些技术和方法，采取这些技术和方法有何优点？

3. 分析你采取上述技术、方法的效果如何，还有哪些需要进一步改进之处以及如何进行改进。

写作要点

1. 论文论述的是电子政务专用网络，而不是常规的局域网或广域网的规划与设计，要体现出电子政务应用背景。

2. 叙述自己参与设计和实施的电子政务专用网络项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量。能够全面和准确地描述该电子政务专用网络的应用环境和需求，深入地阐述规划与设计的主要内容、采用了哪些技术和方法，这些技术和方法要针对电子政务专用网络的特点，具有一定的广度和深度。主要应包括以下内容：

（1）电子政务核心网络规划与设计（重点）。

① 电子政务网络平台构成、IP 地址规划及域名规划、路由策略、组播方案设计、MPLS/VPN 组网、QoS 及流量工程设计等；

② 电子政务平台中各单位接入方式、远程和移动用户接入方式；

③ 网管中心方案、网管中心接入设计、网络管理系统设计。

（2）传输线路规划与设计。

（3）主机与存储系统规划与设计。

① 主机系统设备选型与配置规划；

② 存储系统分析、设计与规划。

（4）容灾与备份系统规划与设计。

① 备份系统建设分析、备份产品选型、备份策略和数据备份的管理等；

② 容灾建设策略、容灾系统设计等。

（5）网络安全的规划与设计。网络隔离方式与规划设计、网络监控与入侵防范、网络漏洞扫描、抗 DDoS 攻击和基于 PKI 的 CA 认证等。

3．对需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

试题二　论网络系统的安全设计

网络的安全性及其实施方法是网络规划中的关键任务之一，为了保障网络的安全性和信息的安全性，各种网络安全技术和安全产品得到了广泛使用。

请围绕“网络系统的安全设计”论题，依次对以下三个方面进行论述。

1．简述你参与设计的网络安全系统以及你所担任的主要工作。

2．详细论述你采用的保障网络安全和信息安全的技术和方法，并着重说明你所采用的软件、硬件安全产品以及管理措施的综合解决方案。

3．分析和评估你所采用的网络安全措施的效果及其特色，以及相关的改进措施。

写作要点

1．论文叙述自己参与设计和实施的网络应用系统应有一定的规模，自己在该项目中担任的主要工作应有一定的分量。

2．能够全面和深入地论述采用的保障网络安全和信息安全的技术和方法，从软件、硬件以及管理措施等多个角度进行说明，具有一定的广度和深度。主要从以下几个方面进行论述：

（1）网络平台及计算机系统的物理安全。

（2）网络平台的数据链路安全。

（3）主要网络安全技术和方法。物理隔离技术、防火墙、网络监控与入侵防范、网络漏洞（弱点）扫描、抗 DDoS 攻击和安全黑洞等。

（4）系统平台安全。操作系统安全、应用软件和数据库系统安全、系统安全管理和系统病毒防范。

（5）网络应用系统安全。防网页篡改、反垃圾邮件等。

（6）可靠性与容错容灾安全。

（7）数据安全。数据传输安全、数据存储安全等。

（8）基于 PKI 的 CA 认证。认证中心、注册登记机构 RA、PKI/CA 建设思路。

（9）安全管理制度。建立完善的安全管理组织机构、安全评估的管理、具体安全策略的管理、工程实施的安全管理、接入管理、建立完善的安全管理制度、运行管理、应急处理、联合防护等。

3．对需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

第 4 章　2010 上半年网络规划设计师上午试题分析与解答

试题（1）

E1 线路是一种以时分多路复用技术为基础的传输技术，其有效数据率（扣除开销后的数据率）约为__（1）__Mbps。

（1）A．1.344　　B．1.544　　C．1.92　　D．2.048

试题（1）分析

本题考查 E1 线路的复用方式方面的基础知识。

E1 线路采用的时分多路复用方式，将一帧划分为 32 个时隙，其中 30 个时隙发送数据，2 个时隙发送控制信息，每个时隙可发送 8 个数据位，要求每秒钟发送 8 000 帧。E1 线路的数据率为 2.048Mbps，每帧发送有效数据的时间只有 30 个时隙，因此有效数据率为（30/32）×2.048Mbps=1.92Mbps。

参考答案

（1）C

试题（2）、（3）

两个节点通过长度为 L（米）、数据率为 B（bps）、信号传播速度为 C（米/秒）的链路相连，要在其间传输长度为 D（位）的数据。如果采用电路交换方式，假定电路的建立时间为 S（秒），则传送全部数据所需要的时间为__（2）__。如果采用分组交换方式，假定分组的长度为 P（位），其中分组头部长度为 H（位），采用连续发送方式。忽略最后一个分组填充的数据量，要使电路交换方式的传送时间小于分组交换方式的传送时间，则应满足的条件是__（3）__。

（2）A．L/C　　B．D/B+L/C
　　C．S+L/C　　D．S+D/B+L/C

（3）A．S<L/C　　B．S<D*H/(B*(P–H))
　　C．D/B<P/H　　D．L/C<P/B

试题（2）、（3）分析

本题考查交换方式的基础知识。

对电路交换方式，发送数据的时间为 D/B，信号从发送端到达接收端经过的传播延迟为 L/C，所以需要的总时间为 S+D/B+L/C。

对分组交换方式，需要计算每个分组的传输时间。分组的个数为 D/(P–H)（不计最后一个分组填充的数据量），发送的总长度为 P*D/(P–H)，需要的发送时间为(P* D/(P–H))/B，信号的传播延迟为 L/C，需要的总时间为(P*D/(P–H))/B+L/C。由 S+D/B+L/C<(P* D/(P–H))/B+L/C，得到 S<D*H/(B*(P–H))。

参考答案

（2）D　（3）B

试题（4）

曼彻斯特编码和 4B/5B 编码是将数字数据编码为数字信号的常见方法，后者的编码效率大约是前者的__（4）__倍。

（4）A．0.5　　B．0.8　　C．1　　D．1.6

试题（4）分析

本题考查数据编码与调制方面的基础知识。

曼彻斯特编码是用两个脉冲编码一个位，其效率为 50%。4B/5B 编码是用 5 个脉冲编码 4 个位，其效率为 80%。

参考答案

（4）D

试题（5）、（6）

万兆局域以太网帧的最短长度和最长长度分别是__（5）__字节。万兆以太网不再使用 CSMA/CD 访问控制方式，实现这一目标的关键措施是__（6）__。

（5）A．64 和 512　　B．64 和 1518　　C．512 和 1518　　D．1518 和 2048

（6）A．提高数据率　　B．采用全双工传输模式

　　C．兼容局域网与广域网　　D．使用光纤作为传输介质

试题（5）、（6）分析

本题考查局域网的基本原理。

传统以太网（10Mbps）采用 CSMA/CD 访问控制方式，规定帧的长度最短为 64 字节，最长为 1518 字节。最短长度的确定，能确保一个帧在发送过程中若出现冲突，则一定能够发现该冲突。发展到千兆以太网，因数据率提高，如果维持帧的最短长度不变，则 CSMA/CD 就会出错，因此将帧的最短长度调整为 512 字节。万兆以太网保持帧长度与千兆以太网一致，所以帧的最短长度和最长长度分别为 512 字节、1518 字节。

万兆以太网不再使用 CSMA/CD，其原因是：万兆以太网采用全双工传输模式，不再保留半双工模式，这样发送和接收使用不同的信道，借助交换机的缓存技术，从微观上消除了冲突，因而不需要 CSMA/CD 来避免冲突。

参考答案

（5）C　（6）B

试题（7）

802.11n 标准规定可使用 5.8GHz 频段。假定使用的下限频率为 5.80GHz，则为了达到标准所规定的 300Mbps 数据率，使用单信道条件下，其上限频率应不低于__（7）__GHz。

（7）A．5.95　　B．6.1　　C．6.4　　D．11.6

试题（7）分析

本题考查信道容量方面的基本知识及奈奎斯特第一定理的应用。

根据奈奎斯特准则，无噪声有限带宽信道的极限容量为 $2W\log_2 v$。但对实际传输系统，该极限值无法达到。奈奎斯特第一定理则从实用的角度给出了带宽与信道数据率的关系，即为了确保信号的传输质量，1bps 需要 2Hz 的带宽。对本题而言，300Mbps 需要 600MHz 即 0.6GHz 的带宽，因此上限频率为 6.4GHz。

参考答案

（7）C

试题（8）

用户要求以最低的成本达到划分 VLAN 的目的，且不能以 MAC 地址作为依据，规划师在规划 VLAN 时，最可能采用的方法是__（8）__。

（8）A．采用具有 VLAN 功能的二层交换机，按端口划分 VLAN

B．采用无网管功能的普通交换机，按 IP 地址划分 VLAN

C．采用具有 IP 绑定功能的交换机，按 IP 地址划分 VLAN

D．采用具有 VLAN 功能的三层交换机，按端口划分 VLAN

试题（8）分析

本题考查 VLAN 及交换机方面的基本知识。

划分 VLAN 的常用方法有按 MAC 地址划分、按交换机端口划分、按 IP 地址划分、按协议划分、按策略划分、按上述方式的组合方式划分等。在工程上，满足本题要求的最可能方式就是采用廉价的具有 VLAN 功能的二层交换机，按端口划分 VLAN。

参考答案

（8）A

试题（9）

存储转发方式是实现网络互联的方式之一，其主要问题是在每个节点上产生不确定的延迟时间。克服这一问题的最有效方法是__（9）__。

（9）A．设置更多的缓冲区　　B．设计更好的缓冲区分配算法

C．提高传输介质的传输能力　　D．减少分组的长度

试题（9）分析

本题考查交换方式、拥塞控制方面的基本知识。

存储转发方式下，减少分组的长度显然不能解决延迟问题。设计更多的缓冲区，实际上可能增加了延迟时间，好的缓冲策略有助于减少排队时间，但效果有限。提高传输介质的传输能力，使得接收到分组后能及时地从输出介质上传送出去，是减少延迟的最有效措施。

参考答案

（9）C

试题（10）

链路状态路由算法是 OSPF 路由协议的基础，该算法易出现不同节点使用的链路状态信息不一致的问题。为解决该问题，可采用的方法是__（10）__。

（10）A．每个节点只在确认链路状态信息一致时才计算路由

B．每个节点把自己的链路状态信息只广播到邻居节点

C．每个节点只在自己的链路状态信息发生变化时广播到其他所有节点

D．每个节点将收到的链路状态信息缓存一段时间，只转发有用的链路状态信息

试题（10）分析

本题考查路由算法方面的基本知识。

链路状态路由算法规定每个节点需要将其链路状态信息广播到所有节点。显然，其他节点不可能同时接收到这个广播信息，因而不同节点保存的链路信息（即网络拓扑）可能不一致，导致计算的路由出现差错。A、B 显然不能解决所述问题。C 减少了发送链路信息的次数，并不能解决所述问题。

每个节点在收到其他节点广播的链路状态信息后，缓存一段时间，在该段时间内，如果收到同一节点发送的新的链路状态信息，则不需要转发旧的链路状态信息。同时，可以将来自多个节点的链路状态信息合并在一起发送。这样能更有效地减少链路状态信息的广播，因而减少因不同的广播导致的不一致问题。

参考答案

（10）D

试题（11）

SDH 网络采用二维帧结构，将 STM-1 帧复用成 STM-4 帧的过程可简述为＿（11）＿。

（11）A．将 4 个 STM-1 帧的头部和载荷分别按字节间插方式相对集中在一起作为 STM-4 帧的头部和载荷，头部的长度占帧长的比例不变

B．将 4 个 STM-1 帧顺序排列，封装成一个 STM-4 帧，头部的长度占帧长的比例不变

C．将 4 个 STM-1 帧的头部和载荷分别集中在一起，头部的长度占帧长的比例不变

D．选取一个 STM-1 帧的头部作为 STM-4 的头部，将 4 个 STM-1 的载荷顺序集中作为 STM-4 的载荷

试题（11）分析

本题考查 SDH 网络的基本知识。

STM-1 的帧格式如图 1 所示。

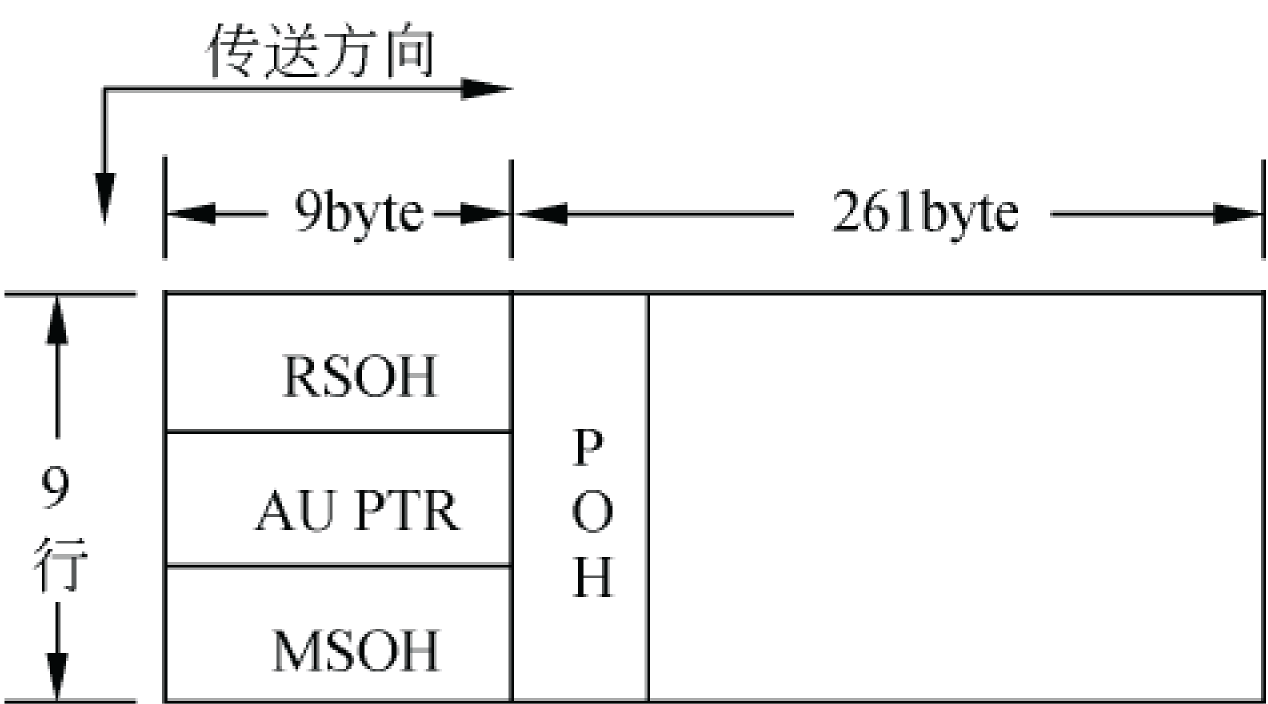


图 1　STM-1 帧结构

SDH 网络规定，将 STM-1 帧复用成 STM-4 帧时，将 4 个 STM-1 帧的头部和载荷分别按字节间插方式相对集中在一起作为 STM-4 帧的头部和载荷，STM-1 的帧头部为 9 列×9 行，共 81 字节。组成 STM-4 帧后，其头部为（4×9）列×9 行，共 324 字节。相应

地，载荷部分为（4×261）列×9 行，其帧格式如图 2 所示。

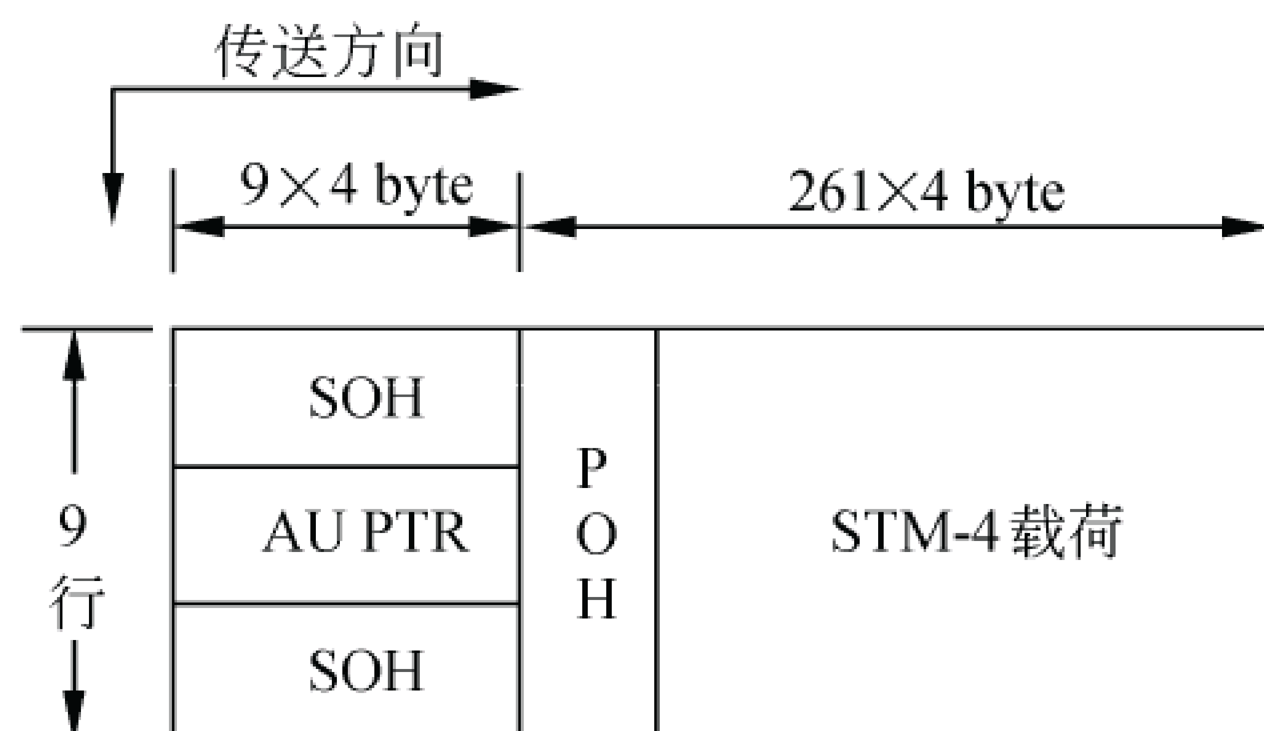


图 2　STM-4 帧结构

参考答案

（11）A

试题（12）

利用 WiFi 实现无线接入是一种广泛使用的接入模式，AP 可以有条件地允许特定用户接入以限制其他用户。其中较好的限制措施是__（12）__。

（12）A．设置 WAP 密钥并分发给合法用户

B．设置 WEP 密钥并分发给合法用户

C．设置 MAC 地址允许列表

D．关闭 SSID 广播功能以使无关用户不能连接 AP

试题（12）分析

本题考查 AP 的基本知识。

AP 限制或允许特定用户接入的主要措施包括密钥认证、MAC 地址过滤、IP 地址过滤等。

密钥认证的基本原理是在 AP 上设置一个密钥，并分发给合法用户。用户在与 AP 建立连接时，需提供密钥供 AP 认证，只有提供的密钥与 AP 上的密钥一致，才能建立连接，AP 才能为用户提供接入服务。主要的密钥认证协议有 WEP、WPA/WPA2、WPA-PSK/WPA2-PSK。

MAC 地址过滤的原理是在 AP 上配置 MAC 地址表，可以是允许表，也可以是禁止表。只有通过 AP 认证的 MAC 地址（也即相应的用户计算机）才能通过 AP 实现接入，其他地址的数据包都会被 AP 丢弃，不转发。

关闭 SSID 广播功能，会使得所有用户都不能连接 AP，因而事实上是关闭了无线功能。

需要说明的是，本题的选项 A 中出现的是 WAP，与 WPA 非常相似，是故意用于迷

惑考生的。WAP 是一种手机传输协议（类似于 HTTP，非安全协议），有些考生可能会认为 WEP 是唯一的密钥协议，因此会选 B。如果将 A 的 WAP 改为 WPA，存在两种密钥协议，性质一样，考生自然会采用排除法，只能选择 C。

在 B 和 C 之间，应选择 C 的原因是，使用密钥认证需要将密钥分发给所有用户，而用户可能一传十、十传百，导致所有人都知道了密钥，失去了限制作用。

参考答案

（12）C

试题（13）、（14）

设计一个网络时，拟采用 B 类地址，共有 80 个子网，每个子网约有 300 台计算机，则子网掩码应设为__（13）__。如果采用 CIDR 地址格式，则最可能的分配模式是__（14）__。

（13）A．255.255.0.0　　B．255.255.254.0

C．255.255.255.0　　D．255.255.255.240

（14）A．172.16.1.1/23　　B．172.16.1.1/20

C．172.16.1.1/16　　D．172.16.1.1/9

试题（13）、（14）分析

本题考查 IP 地址的基本知识。

IP 地址由网络地址和主机地址两部构成，主机地址可进一步划分为子网号和主机号两部分，三者的区分需借助子网掩码实现。

B 类地址的网络地址部分为 2 字节，主机地址（子网号和主机号）为 2 字节。要求有 80 个子网，则子网号部分至少需要 7 位，每个子网能容纳 300 台计算机，则主机号部分至少需要 9 位，A、C、D 显然不能满足要求。

CIDR 地址采用“首地址/网络前缀长度”的形式表示，即 32-网络前缀长度等于网络内的主机地址数，一般按需分配，使得前缀位数尽量大，以节约地址。对本地，地址部分 9 位即可，因此前缀长度为 23 位。

参考答案

（13）B　（14）A

试题（15）

在 IPv6 协议中，一台主机通过一个网卡接入网络，该网卡所具有的 IPv6 地址数最少为__（15）__个。

（15）A．1　　B．2　　C．3　　D．4

试题（15）分析

本题考查 IPv6 的基本内容。

IPv6 规定每个网卡最少有 3 个 IPv6 地址，分别是链路本地地址、全球单播地址和回送地址，这些地址都可以是自动分配的。链路本地地址用于在链路两端传输数据，类似于（但不完全等同于）IPv4 的私用 IP 地址。全球单播地址用于在 Internet 上传输数据，

类似于 IPv4 中的合法的公网 IP 地址。回送地址用于网络测试，类似于 IPv4 的 127.0.0.1。

参考答案

（15）C

试题（16）

利用 ICMP 协议可以实现路径跟踪功能。其基本思想是：源主机依次向目的主机发送多个分组 P1、P2、…，分组所经过的每个路由器回送一个 ICMP 报文。关于这一功能，描述正确的是（16）。

（16）A. 第 i 个分组的 TTL 为 i，路由器 Ri 回送超时 ICMP 报文
B. 每个分组的 TTL 都为 15，路由器 Ri 回送一个正常 ICMP 报文
C. 每个分组的 TTL 都为 1，路由器 Ri 回送一个目的站不可达的 ICMP 报文
D. 每个分组的 TTL 都为 15，路由器 Ri 回送一个目的站不可达的 ICMP 报文

试题（16）分析

本题考查 ICMP 的基本内容。

利用 ICMP 协议实现路径跟踪时，源主机依次向目的主机发送多个分组 P1、P2、…，第 i 个分组 Pi 的 TTL 设为 i，这样 Pi 到达路由器 Ri 时 TTL 变为 0，被 Ri 丢弃，回送超时 ICMP 报文。源节点依据所收到的超时报文的地址，可以组成一条完整的路径，从而实现路径跟踪。

参考答案

（16）A

试题（17）

OSPF 协议规定，当 AS 太大时，可将其划分为多个区域，为每个区域分配一个标识符，其中一个区域连接其他所有的区域，称为主干区域。主干区域的标识符为（17）。

（17）A. 127.0.0.1　　B. 0.0.0.0
C. 255.255.255.255　　D. 该网络的网络号

试题（17）分析

本题考查有关 OSPF 协议的基本知识。

OSPF 协议规定，主干区域连接其他的所有区域，主干区域的标识为 0.0.0.0。

参考答案

（17）B

试题（18）

TCP 协议使用三次握手机制建立连接，其中被请求方在第二次握手时需应答的关键信息及其作用是（18）

（18）A. 确认号是发起方设定的初始序号加 1 之后的数值，确认被请求者的身份
B. 确认号是发起方设定的初始序号+1，确认发起方的身份
C. 确认号是被请求者设定的初始序号+1，同步将要接收的数据流编号
D. 确认号是被请求者设定的初始序号+1，确认发起方的身份

试题（18）分析

本题考查 TCP 协议建立连接的基本知识。

TCP 建立连接采用三次握手的机制，其过程如图 3 所示。

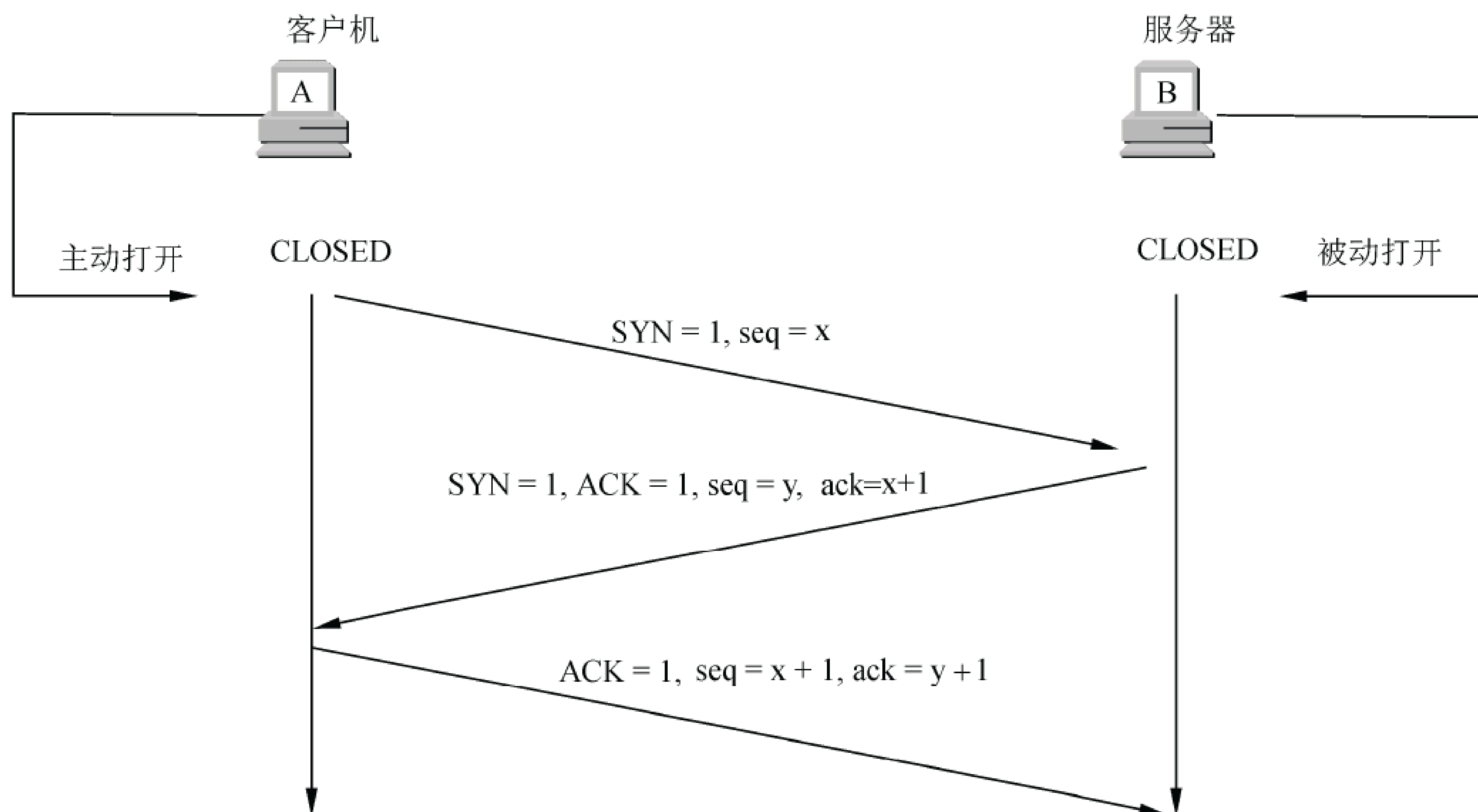


图 3　三次握手

服务器应答的信息中，ack=x+1 中的 x 是发起方设定的一个初始序号，应答方应答此序号表明应答者确实收到了发起方的信息，据此预防冒充者应答，因冒充者收不到发起方的报文，不知道 x 的值。

参考答案

（18）A

试题（19）

由 10 个 AS 连接组成的网络，使用 BGP-4 进行 AS 之间的路由选择。以下叙述正确的是<u>（19）</u>。

（19）A．AS 之间的路由选择由边界路由器完成，选择的输出路由是下一个边界路由器的地址

B．AS 之间的路由选择由 BGP 发言人完成，选择的输出路由包含路径上所有 BGP 发言人的地址

C．AS 之间的路由选择由 BGP 发言人完成，选择的输出路由是下一个网络的地址

D．AS 之间的路由选择由边界路由器完成，选择的输出路由包含所有边界路由器的地址

试题（19）分析

本题考查 BGP 协议及路由的基本知识。

AS 之间采用距离路径路由协议，所选择的路由包含路径上的全部节点，而非距离向量路由协议那样只有下一跳节点。BGP-4 协议是目前用于 AS 之间进行路由选择的路由协议，在每个 AS 内选择 1 个边界路由器，负责本 AS 与其他 AS 之间的路由选择，称为 BGP 发言人。所选择的路由一系列 BGP 发言人构成，这样构成 AS 之间的完整路径。

参考答案

（19）B

试题（20）

有人说，P2P 应用消耗大量的网络带宽，甚至占网络流量的 90%。对此的合理解释是__（20）__。

（20）A．实现相同的功能，P2P 方式比非 P2P 方式需要传输更多数据，占用更多的网络带宽

B．实现相同的功能，P2P 方式比非 P2P 方式响应速度更快，需要占用更多的网络带宽

C．P2P 方式总是就近获取所需要的内容，单个 P2P 应用并不比非 P2P 方式占用更多的带宽，只是用户太多，全部用户一起占用的带宽大

D．P2P 方式需要从服务器获取所需要的内容，单个 P2P 应用比非 P2P 方式需要占用更多的带宽

试题（20）分析

本题考查 P2P 的基本知识。

P2P 网络没有集中式的服务器，每台计算机既是客户机，获取信息和服务，又是服务器，为别人提供信息和服务。P2P 网络中用户总是就近获取所需要的内容，信息的传输采用标准的方式进行，因此单个 P2P 用户或应用并不比非 P2P 方式占用更多的带宽，只是用户太多，且大多数情况下，P2P 应用都是视频类的，如电影、电视节目等，数据量大，需要较大的带宽，全部用户加在一起占用的带宽非常大。

参考答案

（20）C

试题（21）

某网络内部计算机采用私有地址，通过一个路由器连接到 Internet。该路由器具有一个合法的 IP 地址，现在要求 Internet 上的用户能访问该内网上的 Web 服务器，则该内网上 DHCP 服务器及路由器应满足的条件是__（21）__。

（21）A．DHCP 服务器为 Web 服务器分配固定 IP 地址，路由器设置地址映射

B．DHCP 服务器为 Web 服务器分配路由器具有的合法 IP 地址，路由器设置地址映射

C．DHCP 服务器为 Web 服务器动态分配 IP 地址，路由器取消 80 端口过滤功能

D．DHCP 服务器为 Web 服务器动态分配 IP 地址，路由器取消 21 端口过滤功能

试题（21）分析

本题考查 NAT、DHCP 协议方面的基本知识。

内部网上的 Web 服务器要被 Internet 上的用户访问，本应有一个合法的公网 IP 地址。现在，分配的是内部地址，不能被 Internet 用户直接识别。解决方法是：以路由器的合法 IP 地址作为 Web 服务器对外提供服务的地址，DHCP 服务器为 Web 服务器分配一个固定的内部 IP 地址，在路由器上设置地址映射，即来自 Internet 的所有 Web 请求，都被映射并转发到某个固定的内部地址。

参考答案

（21）A

试题（22）

使用 SMTP 协议发送邮件时，可以选用 PGP 加密机制。PGP 的主要加密方式是(22)。

（22）A．邮件内容生成摘要，对摘要和内容用 DES 算法加密

B．邮件内容生成摘要，对摘要和内容用 AES 算法加密

C．邮件内容生成摘要，对内容用 IDEA 算法加密，对摘要和 IDEA 密钥用 RSA 算法加密

D．对邮件内容用 RSA 算法加密

试题（22）分析

本题考查 SMTP 协议和 PGP 的基本知识。

PGP 的工作过程如图 4 所示。

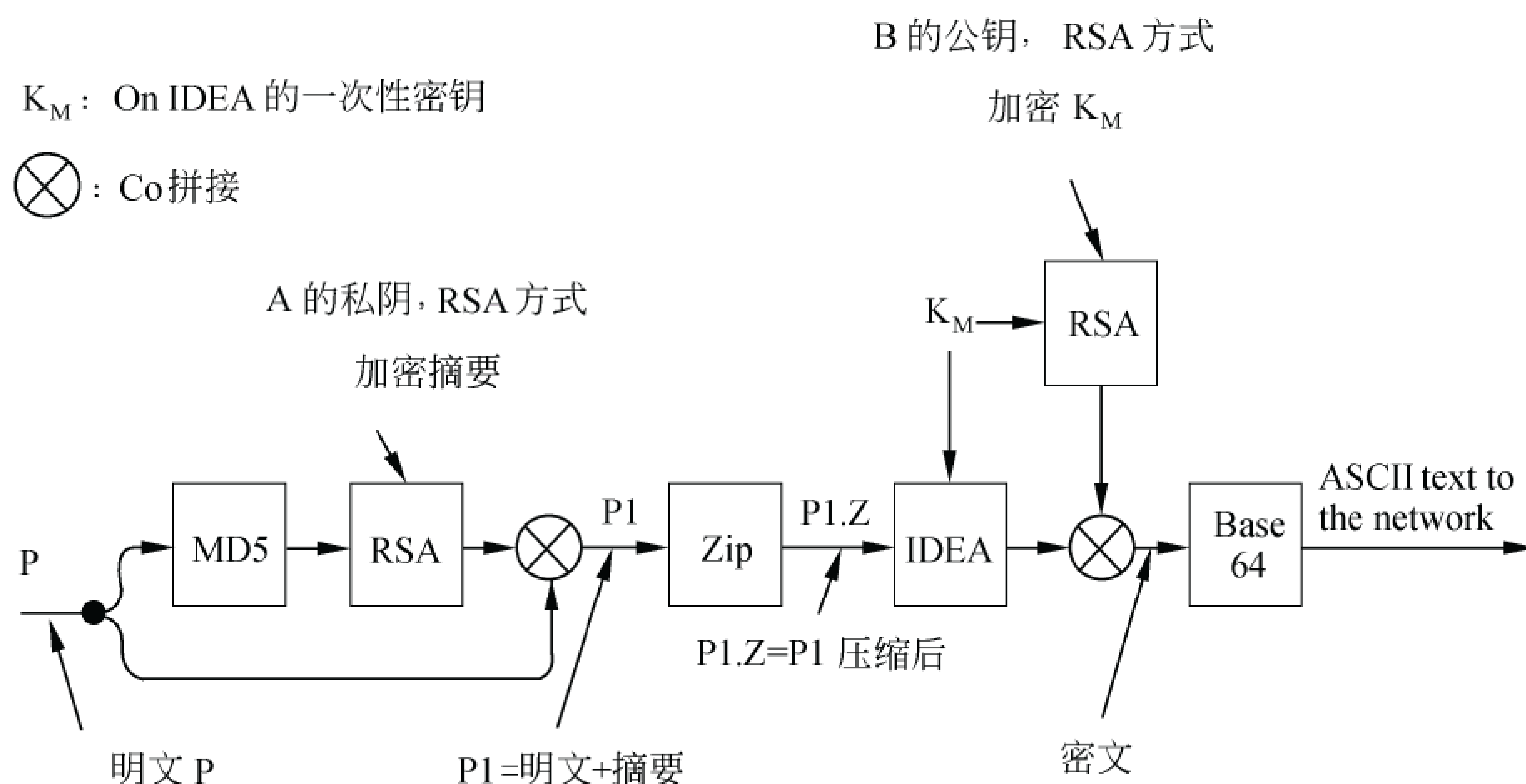


图 4　PGP 工作过程

参考答案

（22）C

试题（23）、（24）

SMI 是 MIB 组织信息的方式，其中每个节点对应一个编码。因第 1 级只有 3 个节点，所以采用了压缩编码。节点 1.3.6.1 对应的压缩编码为<u>（23）</u>；该节点上安装的是 SNMPv2 协议，当该节点出现故障时，网络可能进行的操作是<u>（24）</u>。

（23）A．1.3.6.1　B．0.3.6.1　C．4.6.1　D．43.6.1

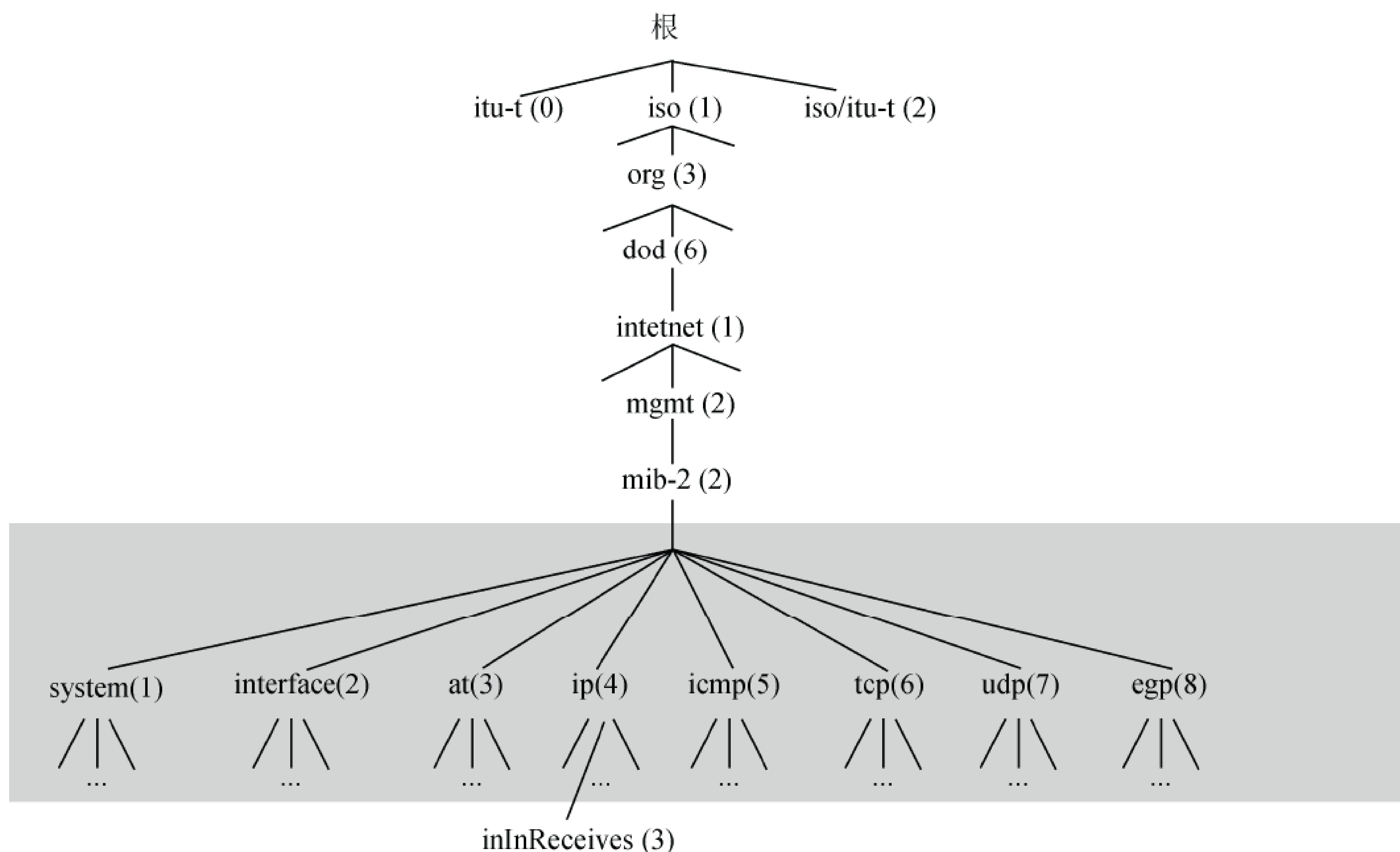
（24）A．故障节点等待 GetRequest 消息　B．故障节点发送 Trap 消息

C．故障节点等待 SetRequest 消息　D．管理节点发送 Trap 消息

试题（23）、（24）分析

本题考查 SNMP、SMI、MIB 方面的基本知识。

SMI 的结构如下图所示。



顶级节点 3 个，下属 2 级节点不超过 39 个，为减少编码长度，将两级合并编码，编码值为 40*X+Y。例如，1.3 编码为 43。所以，节点 1.3.6.1 对应的压缩编码为 43.6.1。

SNMPv2 提供的消息中，只有 Trap 消息是被管节点主动向管理站点发送的消息。当被管节点出现故障时，主动向管理站点发送 Trap 消息以通知故障的存在。

参考答案

（23）D　（24）B

试题（25）、（26）

DiffServ 是 Internet 实现 QoS 的一种方式，它对 IP 的主要修改是<u>（25）</u>，其实现过程可简述为<u>（26）</u>。

（25）A．设置 DS 域，将 IP 分组分为不同的等级和丢弃优先级
B．设置 DS 域和 RSVP 协议
C．定义转发等价类
D．定义多种包格式，分别封装不同优先级的数据

（26）A．边界路由器对数据包进行分类，设置不同的标记，并选择不同的路径 LSP 转发
B．边界路由器对数据包进行分类，设置不同的标识，并根据 SLA 和 PHB 选择不同的队列转发
C．对数据包进行分类，并据此实施资源预留，对不能获得资源的包实施丢弃
D．在网络中设置不同优先级的路径，按照数据包的优先级分别选择相应的路径转发

试题（25）、（26）分析

本题考查 QoS 及 DiffServ 的基本知识。

IP 分组中有 8 位，称为服务类型，定义了优先级（3 位）、延迟、吞吐量、可靠性等 QoS 指标，但网络一直没有使用这些定义。1988 年，将服务类型改为区分服务（DS），用于区分 IP 分组不同的等级及丢弃优先级。

Diffserv 实现 QoS 的基本思想是，边界路由器对数据包进行分类，将 DS 字段设置成不同的标识，并利用 SLA 和 PHB 选择不同的队列转发，以实现有区别的服务，保证高优先级的数据包得到服务质量保证。

参考答案

（25）A　（26）B

试题（27）、（28）

某政府机构拟建设一个网络，委托甲公司承建。甲公司的张工程师带队去进行需求调研，在与委托方会谈过程中记录了大量信息，其中主要内容有：

用户计算机数量：80 台；业务类型：政务办公，在办公时不允许连接 Internet；分布范围：分布在一栋四层楼房内；最远距离：约 80 米；该网络通过专用光纤与上级机关的政务网相连；网络建设时间：三个月。

张工据此撰写了需求分析报告，与常规网络建设的需求分析报告相比，该报告的最大不同之处应该是<u>（27）</u>。为此，张工在需求报告中特别强调应增加预算，以采购性能优越的进口设备。该需求分析报告<u>（28）</u>。

（27）A．网络隔离需求　　B．网络速度需求
C．文件加密需求　　D．邮件安全需求

（28）A．恰当，考虑周全
B．不很恰当，因现有预算足够买国产设备
C．不恰当，因无需增加预算也能采购到好的进口设备

D．不恰当，因政务网的关键设备不允许使用进口设备

试题（27）、（28）分析

本题考查网络工程需求分析的相关知识。

在需求分析阶段，至少应了解业务需求、用户需求、应用需求、平台需求、网络需求、安全需求等基本信息，不同的用户对性能、安全等需求会有所不同。本题涉及的用户是政府机构，其安全性尤其重要，按国家有关规定，政府内网必须采用物理隔离措施与 Internet 隔断，同时，重要部门的安全设备应使用国产设备。

参考答案

（27）A （28）D

试题（29）～（31）

甲方是一个对网络响应速度要求很高的机构，张工负责为甲方的网络工程项目进行逻辑设计，他的设计方案的主要内容可概述为：

① 采用核心层、分布层、接入层三层结构；

② 局域网以使用 WLAN 为主；

③ 骨干网使用千兆以太网；

④ 地址分配方案是：按甲方各分支机构的地理位置划分子网，并按 191.168．n . X 的模式分配，其中 n 为分支机构的序号（0 表示总部，分支机构总数不会超过 10，每个分支机构内的计算机数在 100 至 200 之间）；

⑤ 配置一个具有 NAT 功能的路由器实现机构内部计算机连接 Internet。

针对局域网的选型，你的评价是__（29）__。

针对地址分配方案，你的评价是__（30）__。

针对 NAT 及其相关方案，你的评价是__（31）__。

（29）A．选型恰当

B．不恰当，WLAN 不能满足速度要求

C．不恰当，WLAN 不能满足物理安全要求

D．不恰当，WLAN 不能满足覆盖范围的要求

（30）A．设计合理

B．不合理，子网太多，需要额外的路由器互联

C．不合理，每个子网太大，不利于管理

D．不合理，无法实现自动分配 IP 地址

（31）A．设计合理

B．不合理，计算机太多，NAT 成为瓶颈

C．不合理，不能由一个 NAT 为不同的子网实现地址自动分配

D．不合理，一个路由器不能连接太多的子网

试题（29）～（31）分析

本题考查逻辑网络设计的相关知识。

逻辑网络设计应完成的主要设计包括：网络结构设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理方案设计、网络安全方案设计。

在进行这些方案设计时，应充分考虑性能因素，以确定所选用的技术方案能否满足应用功能和性能的要求。

对本题而言，每个子网由 100～200 台计算机，通过 WLAN 接入，显然不是最佳选择，因 WLAN 在用户多时，速度较慢，难以适应如此大的规模。

采用 192.168 . n . X 的地址模式，划分了很多的子网，需要较多的路由器实现子网之间的互联，一是增加了成本，二是降低了访问速度。因为对于一个公司而言，所有分支机构之间信息共享的要求较高，应减少分隔。

NAT 方式理论上解决了内部计算机访问 Internet 的问题，但当用户较多时，NAT 往往成为网络的瓶颈，导致响应速度极低。

参考答案

（29）B　（30）B　（31）B

试题（32）、（33）

在一个占地 200×80 m^2 生产大型机床的车间里布置网络，有 200 台计算机需要连网，没有任何现成网线，对网络的响应速度要求是能实时控制。设计师在进行物理网络设计时，提出了如下方案：设计一个中心机房，将所有的交换机、路由器、服务器放置在该中心机房，用 UPS 保证供电，用超 5 类双绞线电缆作为传输介质并用 PVC 线槽铺设。该设计方案的最严重问题是__（32）__，其他严重问题及建议是__（33）__。

（32）A．未将机房与厂房分开
　　B．未给出机房的设计方案
　　C．交换机集中于机房浪费大量双绞线电缆
　　D．交换机集中于中心机房将使得水平布线超过 100 米的长度限制

（33）A．普通超 5 类线无抗电磁干扰能力，应选用屏蔽线，用金属管/槽铺设
　　B．PVC 线槽阻燃性能差，应选用金属槽
　　C．超 5 类双绞线性能不能满足速度要求，应改用 6 类双绞线
　　D．生产车间是集中控制，所以应减少计算机数量

试题（32）、（33）分析

本题考查物理网络设计的相关知识。

进行物理网络设计时需要有准确的地形图、建筑结构图，以便规划线路走向、计算传输介质的长度，评估介质布设的合理性，必要时需要计算、评估电磁环境，以确定屏蔽措施。

200×80 m² 的大型车间，设计一个中心机房，所有网络设备全部集中在机房，一定有一些地方离机房的距离超出了 100 米，导致现有方案不能保证所有设备能联网工作。

生产大型机床的车间一定布设了大电流的电力电缆，会产生很强的干扰信号，导致双绞线网络通信电缆上的信号受到严重干扰，网络不能正常工作。

参考答案

（32）D （33）A

试题（34）、（35）

工程师利用某种测试设备在每个信息点对已经连接好的网线进行测试时，发现每个UTP 中都有几根线的长度不正确，以为是 RJ45 接头做得不好，于是重做 RJ45 接头，但现象依旧。经检查，测试设备无故障。其原因是__（34）__，更好的测试方案是__（35）__。

（34）A．测试设备与测试环境不符

B．测试人员不会使用测试设备

C．未连接计算机

D．对端连接了交换机

（35）A．选用更高级的测试设备

B．更换测试人员

C．每个信息点连接计算机看是否能上网

D．用户端不接计算机，在配线间反向测试

试题（34）、（35）分析

本题考查网络的测试方面的基本知识。

网络测试没有现成的标准，通常是一些经验的总结和行业的通用做法。

利用测试设备对 UTP 电缆进行测试时，应将 UTP 对端悬空不连接交换机或计算机，否则，测出的长度数据不正确。

参考答案

（34）D （35）D

试题（36）、（37）

某楼有 6 层，每层有一个配线间，其交换机通过光纤连接到主机房，同时用超 5 类UTP 连接到该楼层的每间房，在每间房内安装一个交换机，连接房内的计算机；中心机房配置一个路由器实现 NAT 并使用仅有的一个外网 IP 地址上联至 Internet；应保证楼内所有用户能同时上网。网络接通后，用户发现上网速度极慢。最可能的原因及改进措施是__（36）__。按此措施改进后，用户发现经常不能上网，经测试，网络线路完好，则最可能的原因及改进措施是__（37）__。

（36）A．NAT 负荷过重。取消 NAT，购买并分配外网地址

B．NAT 负荷过重。更换成两个 NAT

C．路由策略不当。调整路由策略

D．网络布线不合理。检查布线是否符合要求

（37）A．很多人不使用分配的 IP 地址，导致地址冲突。在楼层配线间交换机端口上绑定 IP 地址

B．无法获得 IP 地址。扩大 DHCP 地址池范围或分配静态地址

C．交换机配置不当。更改交换机配置

D．路由器配置不当。更改路由器配置

试题（36）、（37）分析

本题考查网络故障分析与处理方面的基本知识。

网络故障分析与处理的一般思路如图 5 所示。

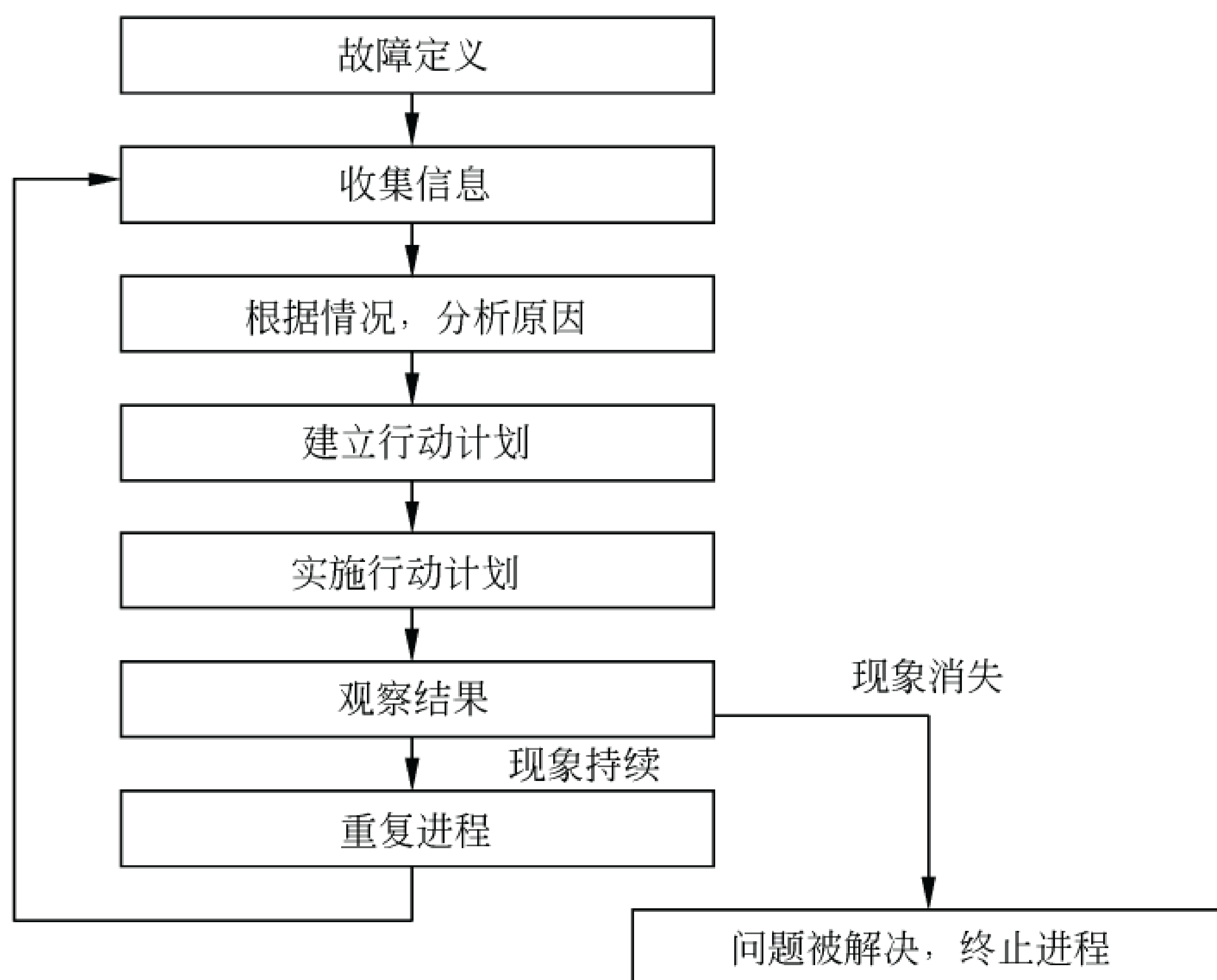


图 5　故障分析与处理模型

其中原因分析、制定行动方案没有标准的模式，在很大程度上依赖人的知识和经验，包括对各类设备、介质、软件等的了解。

针对本题的现象，首先应分析哪些地方可能是网络的瓶颈。显然，楼层交换机、中心机房路由器都是可能的瓶颈，其中 NAT 最有可能成为瓶颈。运行测试软件，可以监测到，路由器的 CPU 利用率极高，可能达到 100%，因此应从 NAT 入手，消除瓶颈。分配静态 IP 地址，即可消除这一瓶颈。

地址盗用是导致所述问题的最可能原因，简单而有效的解决方案如 A 所述。

参考答案

（36）A　（37）A

试题（38）、（39）

评估网络性能时，用户最关心的指标是<u>（38）</u>。当用排队论模型分析网络性能时，

对结果影响最大的参数是（39）。

（38）A. 实际数据率　　B. 丢包率
C. 性价比　　D. 故障率

（39）A. 平均误码率　　B. 分组平均到达率
C. 分组平均长度　　D. 分组平均丢失率

试题（38）、（39）分析

本题考查网络性能评估方面的基本知识。

用户最关心的性能是实际获得的性能，而不是理论值。

网络性能的评估通常先进行理论上的评估，而这需要以一种较好的分析模型和分析方法为基础。排队论模型是用于分析网络性能最经典的理论之一，被广泛应用。其中 M/M/1 模型，是分析分组交换网络性能的主要模型。

参考答案

（38）A　（39）B

试题（40）～（43）

设计师为一个有 6 万师生的大学网络中心机房设计的设备方案是：数据库服务器选用高性能小型机，邮件服务器选用集群服务器，20TB FC 磁盘阵列作为邮件服务器的存储器；边界路由器选用具有万兆模块和 IPv6 的高性能路由器，使用中国电信的 1000Mbps 出口接入到 Internet；安装 500 用户的高性能 VPN 用于校外师生远程访问；使用 4H UPS 作为应急电源。

针对服务器方案，你的评价是（40）。

针对 VPN 方案，你的评价是（41）。

针对接入 Internet 方案，你的评价是（42）。

针对 UPS 方案，你的评价是（43）。

（40）A. 数据库服务器选择恰当，邮件服务器选择不当
B. 数据库服务器选择不当，邮件服务器选择恰当
C. 数据库服务器和邮件服务器均选择恰当
D. FC 磁盘阵列选择不当，应选用 iSCSI 方式

（41）A. VPN 选择规模适当
B. VPN 规模偏大，浪费资源
C. VPN 规模偏小，难以满足要求
D. 不能确定

（42）A. 方案恰当
B. 路由器选择恰当；出口带宽偏小，难以满足要求
C. 路由器配置偏高；出口带宽可行
D. 路由器配置偏高；出口带宽偏小，难以满足要求

（43）A．方案恰当

B．UPS 电池容量偏大，应配备 2H 电池，使用双回路市电

C．UPS 电池容量偏大，应配备 2H 电池，另配一台备用发电机

D．UPS 电池容量太小，应配备 8H 以上电池

试题（40）～（43）分析

本题考查重要的网络资源设备及机房设计的有关知识。

高性能服务器主要有 SMP 结构、MPP 结构、集群结构和 Constellation 结构。

数据库管理系统主要是串行处理，应选用适宜进行高速串行运算的服务器，所以应选用 SMP 结构的高性能小型计算机（按传统的分类标准应是大型计算机）。

邮件服务器的部分功能类似数据库服务器，需要将大量邮件保存到邮件数据库中（集中式的文件），存在大量串行操作，因此选用集群计算机不恰当。

6 万规模的学校，住在校外的师生想必不会很少，在选择 VPN 时，应准确掌握校外师生的规模，以确定 VPN 可支持的用户数。根据经验，满足这一特定环境的 VPN 支持的用户数应不低于 2000。

任何一所大学，校园网内同时上网的人都很多，尤其是在晚上，通常有几万人同时上网，因此需要有较大的出口带宽。

对供电公司和政府而言，学校一般都不是用电的重点保证单位，因此配备 UPS 是必要的，而且应配备 8H 以上的电池，否则难以应对大多数的停电事件。

参考答案

（40）A　（41）C　（42）B　（43）D

试题（44）、（45）

某银行拟在远离总部的一个城市设立灾备中心，其中的核心是存储系统。该存储系统恰当的存储类型是<u>（44）</u>，不适于选用的磁盘是<u>（45）</u>。

（44）A．NAS　B．DAS　C．IP SAN　D．FC SAN

（45）A．FC 通道磁盘　B．SCSI 通道磁盘　C．SAS 通道磁盘　D．固态盘

试题（44）、（45）分析

本题考查网络资源设备中存储系统方面的基本知识。

存储系统的主要结构有三种：NAS、DAS 和 SAN。

DAS（Direct Attached Storage，直接附加存储），存储设备是通过电缆（通常是 SCSI 接口电缆）直接连接服务器。I/O 请求直接发送到存储设备。DAS 也可称为 SAS（Server-Attached Storage，服务器附加存储）。它依赖于服务器，其本身是硬件的堆叠，不带有任何存储操作系统。

DAS 的适用环境为：（1）服务器在地理分布上很分散，通过 SAN（存储区域网络）或 NAS（网络直接存储）在它们之间进行互连非常困难时；（2）存储系统必须被直接连接到应用服务器（如 Microsoft Cluster Server 或某些数据库使用的“原始分区”）上时；

（3）包括许多数据库应用和应用服务器在内的应用，它们需要直接连接到存储器上时。

NAS（Network Attached Storage，网络附加存储），存储系统不再通过 I/O 总线附属于某个特定的服务器或客户机，而是直接通过网络接口与网络直接相连，由用户通过网络来访问。NAS 实际上是一个带有瘦服务的存储设备，其作用类似于一个专用的文件服务器，不过把显示器、键盘、鼠标等设备省去，NAS 用于存储服务，可以大大降低存储设备的成本，另外 NAS 中的存储信息都是采用 RAID 方式进行管理的，从而可有效地保护数据。用户访问 NAS 同访问一台普通计算机的硬盘资源一样简单，甚至可以通过设置 NAS 设备为一台 FTP 服务器，这样其他用户就可以通过 FTP 访问 NAS 中的资源了。也可以通过网页浏览的方式对 NAS 进行管理。

SAN（Storage Area Network，存储区域网络）是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统。SAN 主要采取数据块的方式进行数据存储，目前主要有 IP SAN 和 FC SAN 两种形式（分别使用 IP 协议和光纤通道）。通过 IP 协议，能利用廉价、货源丰富的以太网交换机、集线器和线缆来实现低成本、低风险基于 IP 的 SAN 存储。光纤通道是一种存储区域网络技术，它实现了主机互连，企业间共享存储系统的需求。可以为存储网络用户提供高速、高可靠性以及稳定安全性的传输。光纤通道是一种高性能，高成本的技术。

由于是远程访问，因此选用 IP SAN 结构是最适合的。

固态盘具有最快的速度，但目前固态盘还有一些技术上的限制，主要表现在两个方面，一是存储容量还不能像磁盘一样大，二是写的次数有限制，远低于磁盘。鉴于此，银行的灾备应用目前还不适于选用固态盘。

参考答案

（44）C （45）D

试题（46）

病毒和木马的根本区别是__（46）__。

（46）A．病毒是一种可以独立存在的恶意程序，只在执行时才会起破坏作用。木马是分成服务端和控制端两部分的程序，只在控制端发出命令后才起破坏作用

B．病毒是一种可以独立存在的恶意程序，只在传播时才会起破坏作用。木马是分成服务端和控制端两部分的程序，一般只在控制端发出命令后才起破坏作用

C．病毒是一种可以跨网络运行的恶意程序，只要存在就有破坏作用。木马是驻留在被入侵者计算机上的恶意程序，一旦驻留成功就有破坏作用

D．病毒是一种可以自我隐藏的恶意程序，木马是不需要自我隐藏的恶意程序

试题（46）分析

本题考查病毒与木马的基本概念。

二者最大区别是，木马是分成两部分的，病毒通常是一个整体。

参考答案

（46）A

试题（47）

内网计算机感染木马后，由于其使用私有地址，木马控制端无法与木马服务端建立联系。此时要使木马发挥作用，可采用的方法是__（47）__。

（47）A．由服务端主动向控制端发起通信
B．由双方共知的第三方作为中转站实现间接通信
C．服务端盗用合法 IP 地址，伪装成合法用户
D．服务端以病毒方式运行，直接破坏所驻留的计算机

试题（47）分析

本题考查木马的基本知识。

木马应付私用地址、防火墙等措施的策略之一是采用反向连接技术，即从木马服务器（被控制端）主动向外发起连接，使得与木马控制端建立连接。

参考答案

（47）A

试题（48）、（49）

VPN 实现网络安全的主要措施是__（48）__，L2TP 与 PPTP 是 VPN 的两种代表性协议，其区别之一是__（49）__。

（48）A．对发送的全部内容加密
B．对发送的载荷部分加密
C．使用专用的加密算法加密
D．使用专用的通信线路传送

（49）A．L2TP 只适于 IP 网，传输 PPP 帧；PPTP 既适于 IP 网，也适于非 IP 网，传输以太帧
B．L2TP 只适于 IP 网，传输以太帧；PPTP 既适于 IP 网，也适于非 IP 网，传输 PPP 帧
C．都传输 PPP 帧，但 PPTP 只适于 IP 网，L2TP 既适于 IP 网，也适于非 IP 网
D．都传输以太帧，但 PPTP 只适于 IP 网，L2TP 既适于 IP 网，也适于非 IP 网

试题（48）、（49）分析

本题考查 VPN 协议方面的基本知识。

VPN 实现安全保证的主要措施之一是对发送的数据帧的载荷部分加密。

L2TP 与 PPTP 是 VPN 的两种代表性协议，都封装 PPP 帧，但 PPTP 只适于 IP 网，

L2TP 既适于 IP 网，也适于非 IP 网。

参考答案

（48）B　（49）C

试题（50）

分别利用 MD5 和 AES 对用户密码进行加密保护，以下叙述正确的是＿（50）＿。

（50）A．MD5 只是消息摘要算法，不适宜于密码的加密保护

B．AES 比 MD5 更好，因为可恢复密码

C．AES 比 MD5 更好，因为不能恢复密码

D．MD5 比 AES 更好，因为不能恢复密码

试题（50）分析

本题考查消息摘要算法和对称加密算法的基本原理。

MD5 是消息摘要算法，用于对消息生成定长的摘要。消息不同，生成的摘要就不同，因此可用于验证消息是否被修改。生成摘要是单向过程，不能通过摘要得到原始的消息。如果用于密码保护，其优点是保存密码的摘要，无法获得密码的原文。AES 是一种对称加密算法，对原文加密后得到密文，通过密钥可以把密文还原成明文。用于密码保护时，有可能对密文实施破解，获得密码的明文，所以其安全性比 MD5 低。

参考答案

（50）D

试题（51）～（53）

RSA 是一种公开密钥加密算法。其原理是：已知素数 p、q，计算 n=pq，选取加密密钥 e，使 e 与(p–1)×(q–1)互质，计算解密密钥 $d \equiv e^{-1} \bmod ((p-1)\times(q-1))$。其中 n、e 是公开的。如果 M、C 分别是明文和加密后的密文，则加密的过程可表示为＿（51）＿。

假定 $E_X^Y(M)$表示利用 X 的密钥 Y 对消息 M 进行加密，$D_X^Y(M)$ 表示利用 X 的密钥 Y 对消息 M 进行解密，其中 Y=P 表示公钥，Y=S 表示私钥。A 利用 RSA 进行数字签名的过程可以表示为＿（52）＿，A 利用 RSA 实施数字签名后不能抵赖的原因是＿（53）＿。

（51）A．$C=M^e \bmod n$　　B．$C=M^n \bmod e$

C．$C=M^d \bmod n$　　D．$C=M^e \bmod d$

（52）A．$E_B^S(E_A^P(M))$　　B．$E_B^P(E_A^S(M))$

C．$E_B^P(E_A^P(M))$　　D．$D_B^P(E_A^P(M))$

（53）A．算法是有效的

B．是 A 而不是第三方实施的签名

C．只有 A 知道自己的私钥

D．A 公布了自己的公钥，且不可伪造

试题（51）～（53）分析

本题考查 RSA 的基本知识。

RSA 的原理如题所述，加密过程是先将明文分成多个组，每组看成一个整数 M，加密就是计算 $C=M^e \bmod n$。

RSA 可以用于数字签名，其过程是：用签名者的私钥对消息加密，然后再用接收者的公钥对加密后的内容加密。因为签名过程中用签名者的私钥对消息进行了加密，且只有签名者本人知道其私钥，因此这样的签名是不能抵赖的。

参考答案

（51）A　（52）B　（53）C

试题（54）、（55）

PKI 由多个实体组成，其中管理证书发放的是__（54）__，证书到期或废弃后的处理方法是__（55）__。

（54）A．RA　　B．CA　　C．CRL　　D．LDAP

（55）A．删除　　B．标记无效

C．放于 CRL 并发布　　D．回收放入待用证书库

试题（54）、（55）分析

本题考查 PKI 的基本知识。

PKI 的系统结构如图 6 所示。

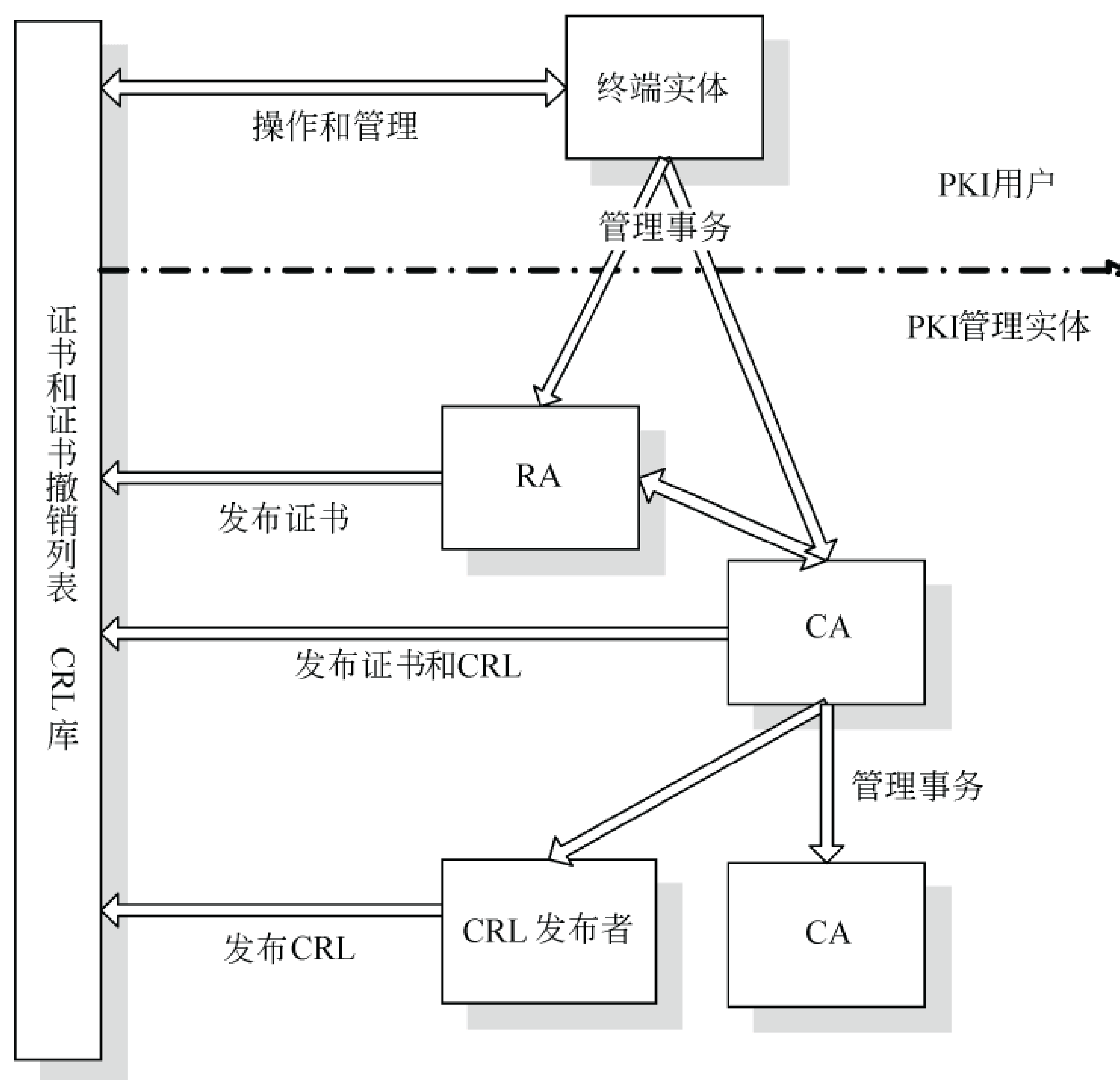


图 6　PKI 系统结构

负责证书发放的是 CA（证书机构），证书到期或废弃后将其放入 CRL（证书撤销列表）。

参考答案

（54）B　（55）C

试题（56）、（57）

甲公司是一个有 120 人的软件公司，为加强安全管理，甲公司对公司内局域网采取了如下措施：安装隔离网闸限制对 Internet 的访问；安装过滤软件禁止邮件被发送到 Internet；对堆叠在一起的 3 台 48 口交换机的每个已连接端口，绑定 MAC 地址和 IP 地址，限制无关计算机访问局域网；每台计算机只安装 DVDROM 并取消 USB 口以防止公司重要文档被拷贝。但公司发现，这些措施没能阻止公司机密文档的泄露。

一个明显且主要的漏洞是 （56） 。

即使没有上述漏洞，员工也可以将自己的笔记本计算机连接到公司局域网上，拷贝相关文档，其可行的手段是 （57） 。

（56）A. 隔离网闸不能阻止信息传送
B. 员工可建立 FTP 服务器外传文档
C. 没有设置进入网络的密码系统
D. 没有限制交换机上未用的端口

（57）A. 秘密修改交换机的配置
B. 盗用别人的密码进入网络
C. 在笔记本计算机上实施 MAC 地址克隆
D. 绕开交换机直接与服务器相连接

试题（56）、（57）分析

本题考查访问控制的基本知识。

题中所述安全措施是一个初级的、具有一定效果的安全方案，但是存在一个明显的漏洞，就是只对已经使用的交换机端口进行了限制，而对交换机上未启用的端口没有限制。这样，员工或其他人就可以将一台计算机连接到一个以前未启用的交换机端口上，自由地访问局域网，拷贝文档。

堵塞上述漏洞后，仍然存在漏洞，即 MAC 地址克隆。这在 Windows 下实施比较容易，只要知道原来每个端口上绑定的是哪个 MAC 地址，就可通过查询正在使用的计算机即可获知。MAC 地址克隆的具体方法此处不作介绍。

参考答案

（56）D　（57）C

试题（58）～（61）

张工组建了一个家庭网络并连接到 Internet，其组成是：带 ADSL 功能、4 个 RJ45 接口交换机和简单防火墙的无线路由器，通过 ADSL 上联到 Internet，家庭内部计算机通过 WiFi 无线连接，一台打印机通过双绞线电缆连接到无线路由器的 RJ45 接口供全家共享。某天，张工发现自己的计算机上网速度明显变慢，硬盘指示灯长时间闪烁，进一步

检查发现，网络发送和接收的字节数快速增加。张工的计算机出现这种现象的最可能原因是__（58）__，由此最可能导致的结果是__（59）__，除了升级杀病毒软件外，张工当时可采取的有效措施是__（60）__。做完这些步骤后，张工开始全面查杀病毒。之后，张工最可能做的事是__（61）__。

（58）A. 感染了病毒　　B. 受到了木马攻击
C. 硬盘出现故障　　D. 网络出现故障

（59）A. 硬盘损坏　　B. 网络设备不能再使用
C. 硬盘上资料被拷贝或被偷看　　D. 让硬盘上的文件都感染病毒

（60）A. 关闭计算机
B. 关闭无线路由器
C. 购买并安装个人防火墙
D. 在无线路由器上调整防火墙配置过滤可疑信息

（61）A. 格式化硬盘重装系统
B. 购买并安装个人防火墙
C. 升级无线路由器软件
D. 检查并下载、安装各种补丁程序

试题（58）～（61）分析

本题考查黑客攻击与预防方面的基本知识。

出现题述现象的原因很多，比如正在进行软件的自动升级，通过网络方式查杀病毒，P2P 方式共享文件，等等。

张工在排除了多种原因之后，剩下最可能的原因就是感染了木马，计算机被控制，不停地向外发送信息，或下载并不需要的文件。

安装个人防火墙具有一定的作用，但如果配置不当，或未准确掌握对方的信息，个人防火墙并不能解决上述问题，况且在上述条件下，也有些多余，因为路由器上已具有基本的个人防火墙。

木马通常是利用各种漏洞来发挥作用的，因此应经常安装补丁程序。

参考答案

（58）B　（59）C　（60）D　（61）D

试题（62）

ACL 是利用交换机实现安全管理的重要手段。利用 ACL 不能实现的功能是__（62）__。

（62）A. 限制 MAC 地址　　B. 限制 IP 地址
C. 限制 TCP 端口　　D. 限制数据率

试题（62）分析

本题考查交换机安全配置方面的基本知识。

ACL（访问控制列表）是交换机实现访问控制的机制，可以实现对网络受限制的访

问。限制数据率也是交换机的功能之一，但不是 ACL 的功能。

参考答案

（62）D

试题（63）、（64）

某公司打算利用可移动的无线传感器组成一个 Ad hoc 式的无线传感器网络，用于野外临时性监控，并把监测结果通过 Internet 传送到公司内部的服务器。适于该网络的路由协议是__（63）__，用于该网络与公司通信的最佳方式是__（64）__。

（63）A. RIP　B. OSPF　C. AODV　D. BGP-4

（64）A. ADSL　B. 3G　C. WiMAX　D. GPRS

试题（63）、（64）分析

本题考查广域网的基本知识。

Ad hoc 网络的典型协议有 AODV、DSR 等。AODV 是 Ad hoc 网络中按需距离向量路由协议的简称，模仿有线网络中的距离向量路由协议，但节点不永久保存路由信息，而是在需要时发起建立路由的过程。

由于该网络部署在野外，且是临时性的，因此优先考虑用无线方式接入到 Internet 或公司的网络。GPRS 虽可用的区域广，但数据率低。WiMAX 还没有被广泛部署。现实条件下只有 3G 是一种好的选择。

参考答案

（63）C　（64）B

试题（65）

进度控制工作包含大量的组织和协调工作，而__（65）__是组织和协调的重要手段。

（65）A. 技术审查　B. 会议　C. 工程付款　D. 验收

试题（65）分析

本题考查项目管理中进度控制的基本知识。

技术审查的目的主要是质量控制。

参考答案

（65）B

试题（66）

在项目施工成本管理过程中，完成成本预测以后，需进行的工作是__（66）__。

其中：①成本计划　②成本核算　③成本控制　④成本考核　⑤成本分析。

（66）A. ①→②→③→④→⑤　B. ①→③→④→②→⑤

C. ①→③→②→⑤→④　D. ①→④→②→③→⑤

试题（66）分析

本题考查成本控制方面的基本知识。

参考答案

（66）C

试题（67）

项目管理方法的核心是风险管理与＿（67）＿相结合。

（67）A．目标管理　B．质量管理　C．投资管理　D．技术管理

试题（67）分析

本题考查项目风险管理的基本知识。

参考答案

（67）A

试题（68）

知识产权可分为两类，即＿（68）＿。

（68）A．著作权和使用权　B．出版权和获得报酬权
C．使用权和获得报酬权　D．工业产权和著作权

试题（68）分析

本题考查知识产权方面的基本知识。

我国知识产权法规定，知识产权可分为工业产权和著作权两类。

参考答案

（68）D

试题（69）

乙公司参加一个网络项目的投标，为降低投标价格以增加中标的可能性，乙公司决定将招标文件中的一些次要项目（约占总金额的 3%）作为可选项目，没有计算到投标总价中，而是另作一张可选价格表，由招标方选择是否需要。评标时，评委未计算可选价格部分，这样乙公司因报价低而中标。实施时，甲方提出乙方所说的可选项是必须的，在招标文件中已明确说明，要求乙方免费完成。针对这些所谓可选项目，最可能的结果是＿（69）＿。

（69）A．在甲方追加经费后乙公司完成
B．乙公司免费完成
C．甲方不追加经费，相应部分取消
D．甲方起诉到法院

试题（69）分析

本题考查项目管理中招投标方面的基本知识。

招标书是描述用户需求的重要文件，无特殊情况时，双方都应以此为依据。由于本题涉及的金额不大，乙方一般会免费完成。

参考答案

（69）B

试题（70）

在采用 CSMA/CD 控制方式的总线网络上，假定τ =总线上单程传播时间，T_0=发送一个帧需要的时间（=帧长/数据率），$a=\tau/T_0$。信道利用率的极限值为__（70）__。

（70）A. $\frac{1}{1+a}$　　B. $\frac{a}{1+a}$　　C. $\frac{a}{1+2a}$　　D. $\frac{1}{1+2a}$

试题（70）分析

本题考查应用数学中概率统计知识的应用。

信道利用率达到极限的条件是：一个节点发送的一个帧到达目的地后，某一个节点接着发送，介质没有空闲，也没有出现冲突的情况。此时，发送 1 帧的时间是 T_0，帧的传播延迟是τ，总时间为 $T_0+\tau$，利用率为 $T_0/(T_0+\tau)=1/(1+a)$。

参考答案

（70）A

试题（71）～（75）

One of the most widely used routing protocols in IP networks is the Routing Information Protocol (RIP). RIP is the canonical example of a routing protocol built on the __(71)__ algorithm. Routing protocols in internetworks differ slightly from the idealized graph model. In an internetwork, the goal of the routers to forward packets to various __（72）__.

Routers running RIP send their advertisement about cost every __（73）__ seconds. A router also sends an update message whenever an update from another router causes it to change its routing table.

It is possible to use a range of different metrics or costs for the links in a routing protocol. RIP takes the simplest approach, with all link costs being equal __（74）__. Thus it always tries to find the minimum hop route. Valid distances are 1 through __（75）__.This also limits RIP to running on fairly small networks.

（71）A. distance vector　　B. link state
　　C. flooding　　D. minimum spanning tree

（72）A. computers　　B. routers
　　C. switches　　D. networks

（73）A. 10　　B. 30
　　C. 60　　D. 180

（74）A. 1　　B. 15
　　C. 16　　D. length of the link

（75）A. 6　　B. 10
　　C. 15　　D. 16

参考译文

IP 网络中广泛使用的路由协议之一是路由信息协议（RIP）。RIP 是基于__（71）__路由算法的路由协议。网络中的路由协议与理想的图算法存在少量的差异。在互联网中，路由器的目的是将数据包转发给不同的__（72）__。

运行 RIP 协议的路由器每__（73）__秒广播一次路由信息，另外，每当路由器收到其他路由器的更新消息而导致其路由表变化时，就会发送更新消息。

路由协议使用不同的度量或成本来建立连接是可能的。RIP 采用了最简单的方法，所有链路的成本都等于__（74）__。这样，它总是试图寻找跳数最少的路径。有效的距离范围是从 1 到__（75）__。这也限制了 RIP 只能在相当小规模的网络上运行。

参考答案

（71）A　（72）D　（73）B　（74）A　（75）C

第 5 章　2010 上半年网络规划设计师下午试卷 I 试题分析与解答

试题一（共 25 分）

阅读以下关于某城市平安城市工程的叙述，回答问题 1、问题 2 和问题 3。

某城市为满足治安管理、城市管理、交通管理、应急指挥等需求，决定在城市的所有进出路口、客货运场所、主要道路路口、重要公共场所、商业密集区域、治安案件高发区等地进行视频监控，并通过网络建立完善的社会治安视频监控系统，即实施“平安城市工程”，实现视频监控信息资源的整合与共享。

平安城市工程的网络接入如图 1-1 所示。

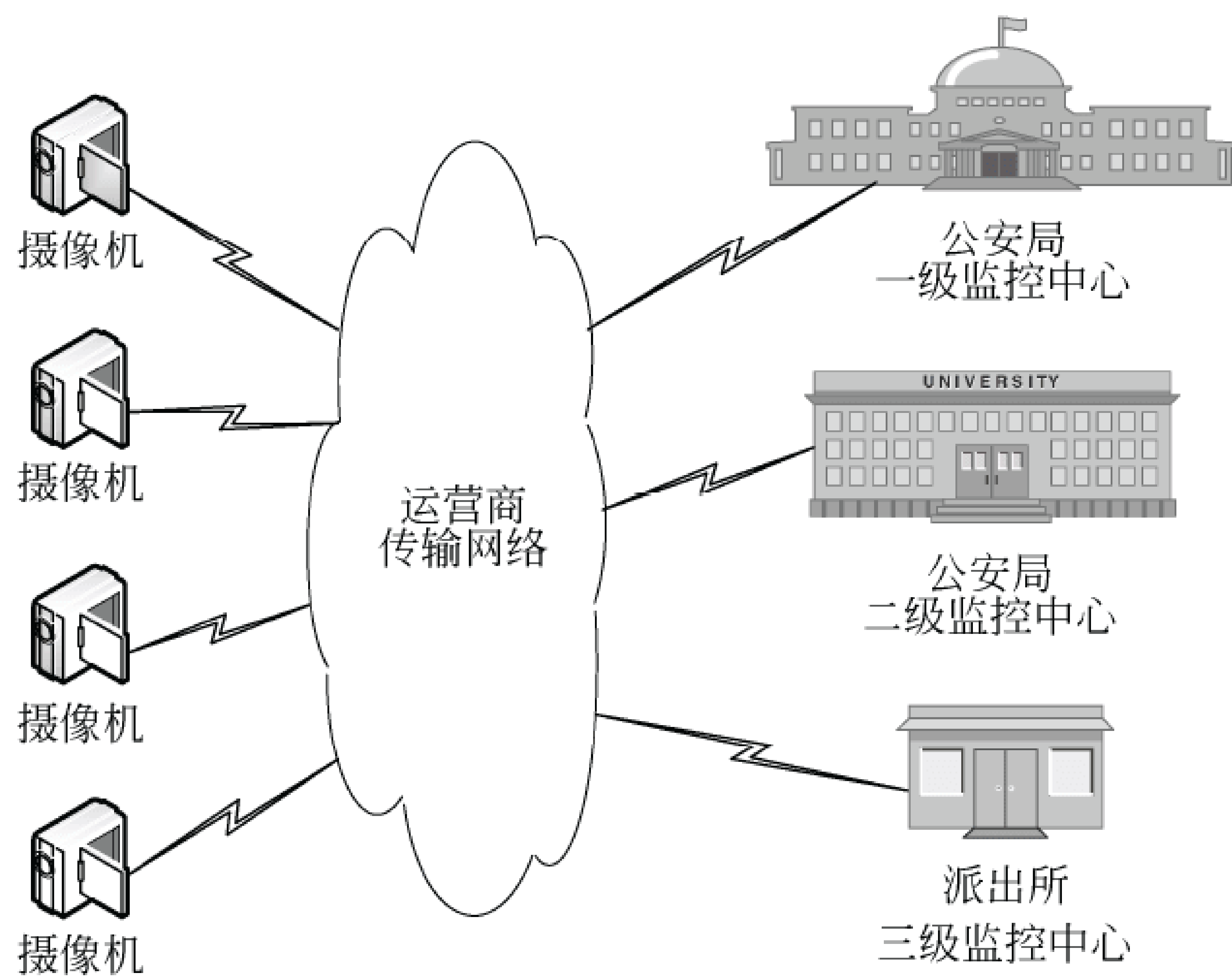


图 1-1　平安城市网络接入

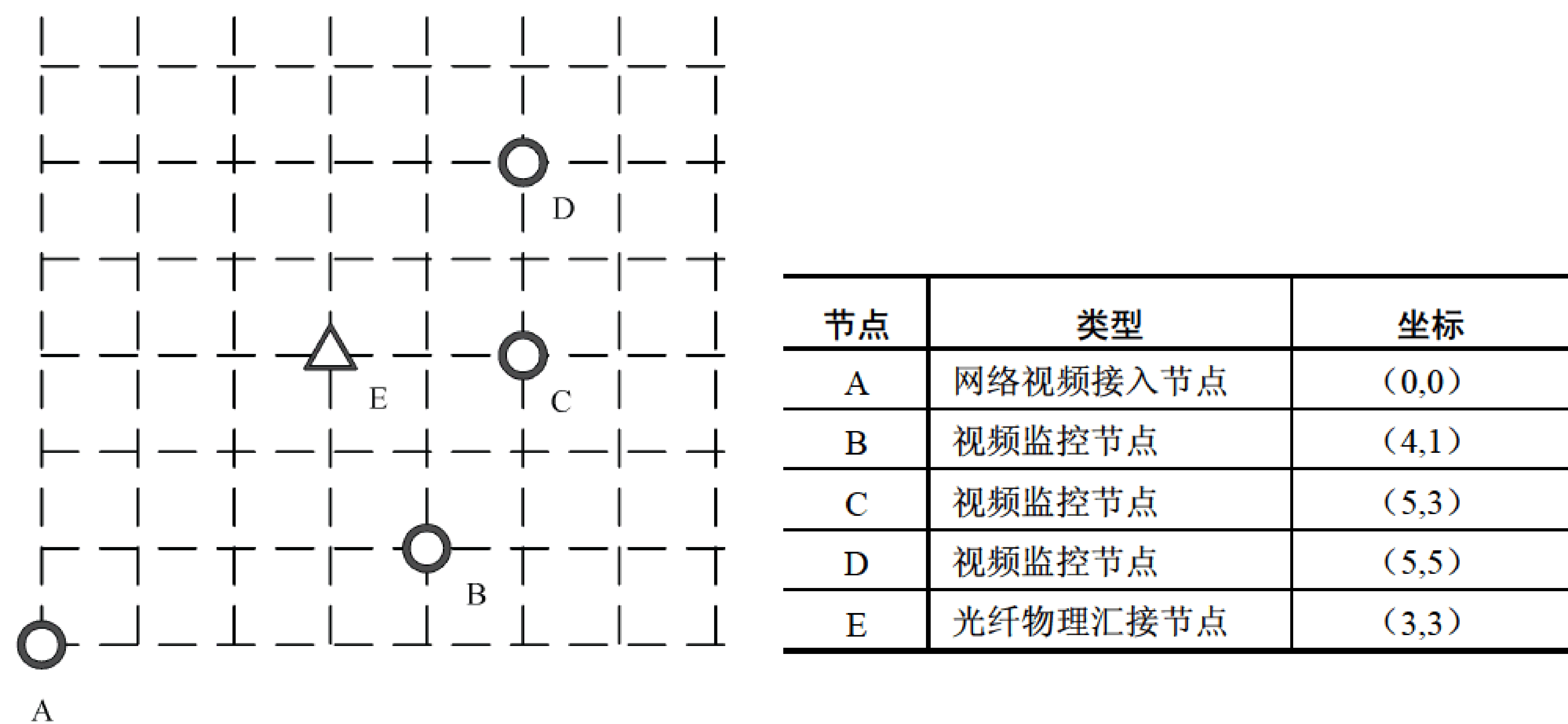
所有监控点的摄像机通过运营商提供的线路接入平安城市网络，公安局的监控体系有三级构成，分别为市局、分局和派出所监控中心。

运营商传输网络负责所有视频监控信号的传输、存储和转发，传输网络由传输设备、网络设备、存储设备等构成。

【问题 1】（6 分）

运营商网络中的某一个网络视频接入节点，需要通过一台交换机实现三个监控点摄像机的视频图像接入，摄像机和交换机之间采用光纤进行互连，并存在一个光纤物理汇

接节点（用于实现光纤的熔接配置）。各节点的类型、分布和位置坐标如图 1-2 所示，允许采用 2 芯、4 芯、8 芯或 16 芯的光缆。请指出采用“网络节点至监控点直埋光纤”、“通过光纤汇接点汇接光纤”和“基于 EPON 分光器互连光纤”三种方式需要埋设的光缆类型并计算所需每种类型光缆的最短长度。（注：在计算长度时，$\sqrt{n}$ 直接可在计算结果中出现。）



节点	类型	坐标
A	网络视频接入节点	（0,0）
B	视频监控节点	（4,1）
C	视频监控节点	（5,3）
D	视频监控节点	（5,5）
E	光纤物理汇接节点	（3,3）

图 1-2　节点分布图

【问题 2】（10 分）

Catalyst 6509 作为整个网络的核心交换设备。

核心交换机 3 号插槽上安装 8 端口 GBIC 千兆以太网模块 WS-X6408A（8 port GIGABIT ETHERNET），端口 1 至 3 分别与行政区甲、行政区乙和行政区丙的汇聚交换机互连，其他端口与各级指挥中心的汇聚交换机互连，核心交换机至行政区甲、乙、丙的距离分别为 8、22 和 42km。表 1-1 列出了光电收发器及配件的参数指标，请从表 1-1 中选择与端口 1、端口 2、端口 3 连接的收发器及配件，并分别指出应采用的光纤链路。

表 1-1　光电收发器配件

序号	产 品 类 型	参 数 指 标	备　注
1	WS-G5484	1000BaseSX，多模光纤链路	短距离通信
2	WS-G5486	1000BaseLX/LH，遵循 IEEE 802.3z 1000BaseLX 标准，使用高质量单模光纤链路可使距离扩充一倍	长距离通信
3	WS-G5487	1000BaseZX，与单模光纤一起使用，普通单模光纤链路上最远可以传递 70km，使用高质量单模光纤链路最远可至 100km	超长距离通信
4	5dB 线上光衰减器	增加 25km 的光信号衰减	避免光收发器过载
5	10dB 线上光衰减器	增加 50km 的光信号衰减	避免光收发器过载

【问题 3】（9 分）

核心交换机 4 号插槽上安装 16 端口 GBIC 千兆以太网模块 WS-X6516-GBIC（16 port GIGABIT ETHERNET），负责连接平安城市工程中所有的流媒体服务器、存储服务器等设备，端口 1 和 2 连接 2 台流媒体服务器、端口 3 和 4 连接 2 台存储服务器。平安城市工程规范中规定，实时调阅视频流从采集至播放的时间延迟不得大于 1s。图 1-3 为某派出所对一个监控点之间的设备连接图，表 1-2 为图中各设备产生的延迟情况。请计算该派出所对监控点的实时视频调阅延迟，并指出是否符合平安城市工程规范；如不符合规范，在不能改变编解码器和流媒体服务器产品的情况下，给出可能的优化方案。

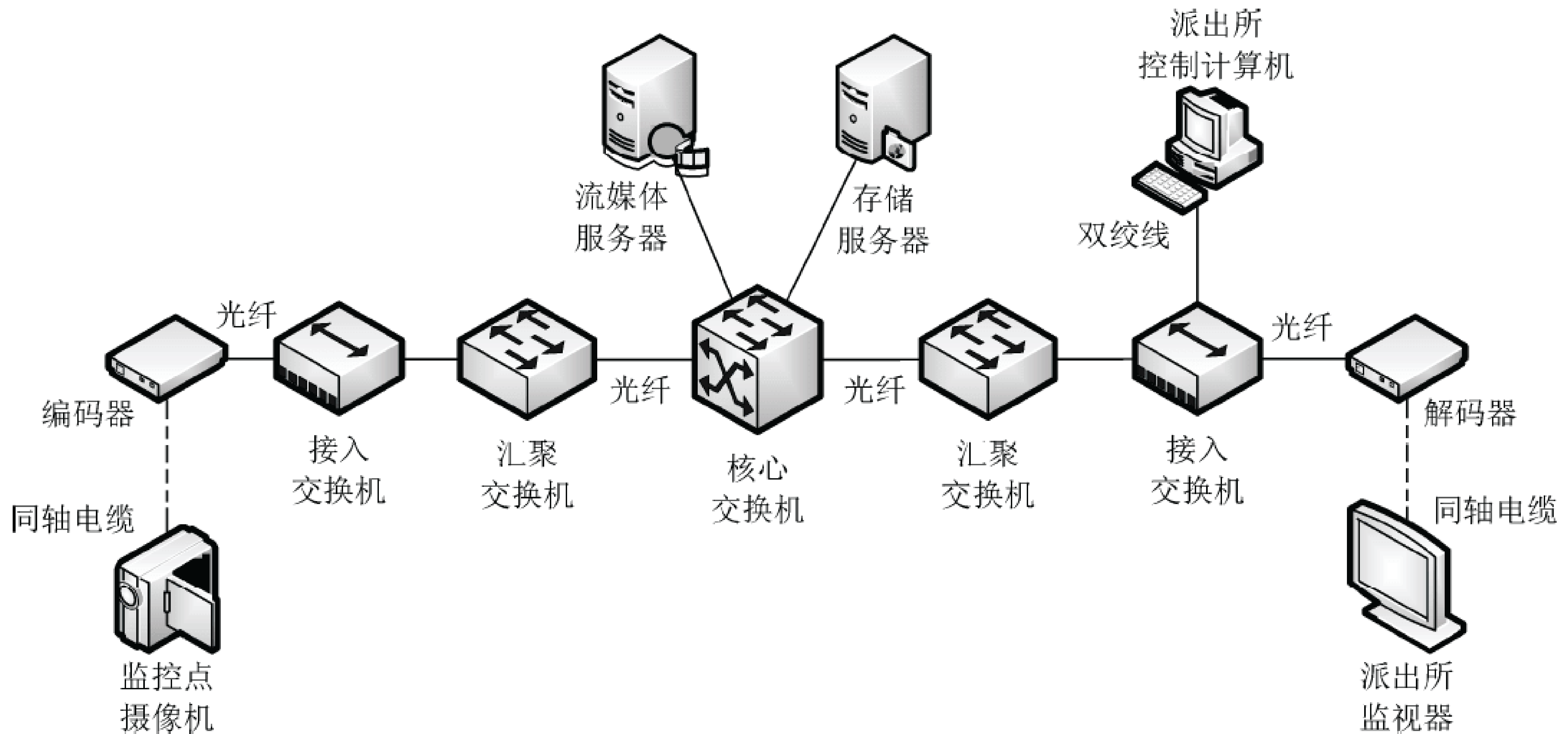


图 1-3 设备连接图

表 1-2 设备延迟情况

序号	设　　备	延 迟 原 因	延迟时间（ms）	备　　注
1	编码器	视频信号模数转换延时	400	
2	接入交换机	数据帧转发延时	30	
3	汇聚交换机	数据帧转发延时	30	
4	核心交换机	数据帧模块间转发延时	10	
5	核心交换机	数据帧模块内端口间转发延时	5	
6	流媒体服务器	视频流处理及转发延时	70	
7	存储服务器	视频存储延时	200	
8	存储服务器	视频调阅转发延时	100	
9	解码器	视频信号数模转换延时	400	
10	各线路	信号传输延时	0	忽略不计

试题一分析

本题涉及光纤铺设、超长距离光电收发器配置、网络延迟等方面的内容。

【问题 1】

本问题主要涉及光纤铺设领域的工程知识。在平安城市工程中，监控点至网络接入层的光纤铺设不仅仅涉及光纤链路的租赁费用，还直接导致工程建设过程中由于光纤铺设而产生破路、回填、修复、绿化等间接成本；因此针对不同的监控点分布，选择合适的光纤铺设方式是至关重要的。

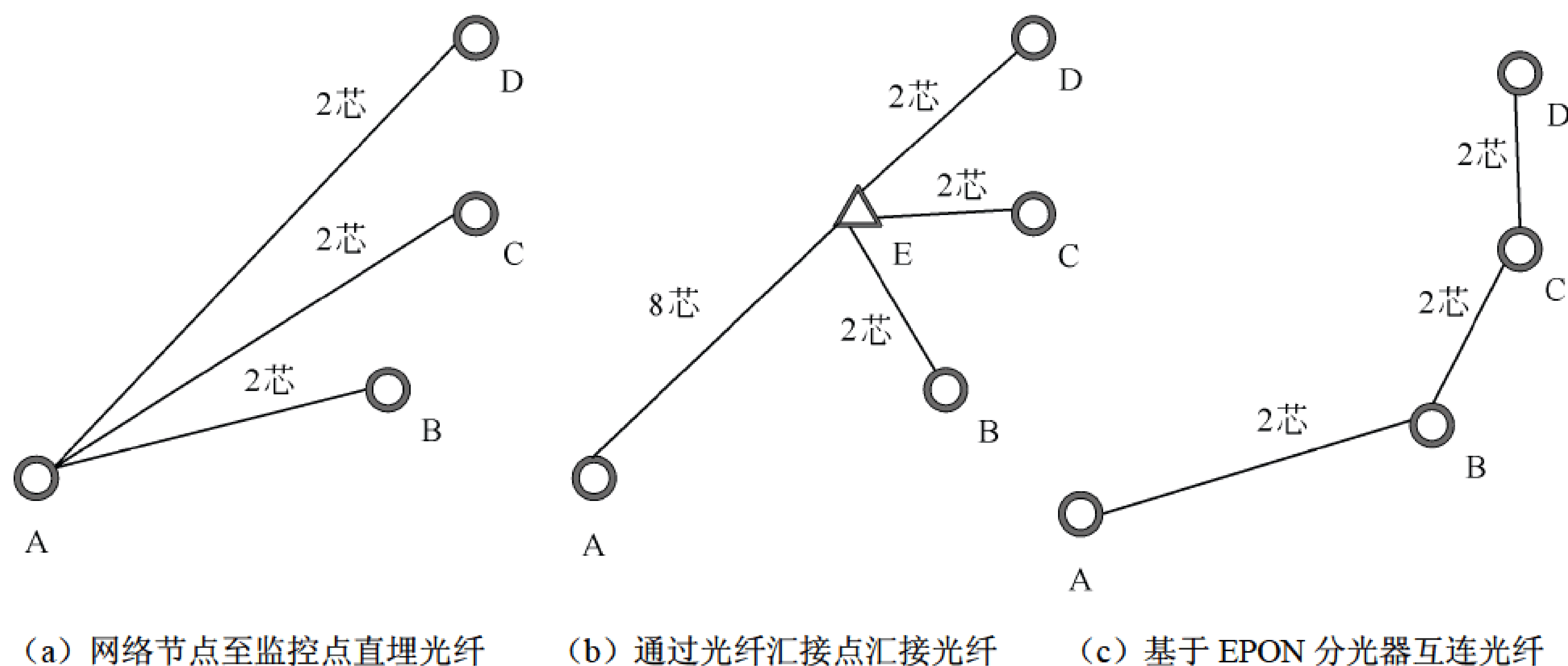
平安城市工程中，各监控点的主要设备为摄像机与视频编码器，视频编码器通过 2 芯光缆与其他节点连接。问题 1 可以采用的三种方式是目前平安城市工程中常见的三种铺设方式。

“网络节点至监控点直埋光纤”指在监控点至网络接入层节点之间直接埋设一根 2 芯光缆，形成网络节点至各监控点的一个中心辐射状物理链路关系。

“通过光纤汇接点汇接光纤”指在网络接入层节点和监控点之外存在一个光纤汇节点，通常情况下网络节点至光纤汇接点之间是一根多芯光缆，而光纤汇接点至各监控点之间为一根 2 芯光缆。在这种方式下，网络节点与各监控点在逻辑上仍然是一个中心辐射关系，网络节点至各监控点的光纤仍为 2 芯；但是从光纤的物理分布上，为了减少光缆铺设工程量，其实已经发生了变化，光纤的割接点不在网络节点，而下移至光纤汇接点。

“基于 EPON 分光器互连光纤”是随着 EPON 技术在平安城市工程的应用而产生的一种光纤铺设方式，EPON 技术采用分光器串联的方式，把所有监控点连接起来，因此在当前技术条件下，当监控节点少于 50 个时，可以用一根 2 芯光缆把所有监控点连接起来。

基于以上分析，结合题设，可以形成如图 1-4 所示的光纤铺设方式。



（a）网络节点至监控点直埋光纤　（b）通过光纤汇接点汇接光纤　（c）基于 EPON 分光器互连光纤

图 1-4　光纤铺设方式

【问题 2】

本问题主要考查在不同传输距离的情况下，如何正确选择光电收发器及其光纤链路。

与大多数网络设备厂商一样，Cisco 公司提供的光电收发器遵循千兆位接口转换器

（GBIC）标准，是一种热插拔的输入输出设备，该设备插入千兆位以太网端口/插槽内，负责将端口与光纤网络连接在一起。GBIC 可以在各种 Cisco 产品上使用和互换，并可逐个端口地与遵循 IEEE 802.3z 的 1000BaseSX、1000BaseLX/LH 或 1000BaseZX 接口混用。

WS-G5484：WS-G5484 模块遵循 1000BaseSX 标准，工作在普通的多模光纤链路上，最大传输距离达 550m。

WS-G5486：WS-G5486 模块是一种完全遵循 IEEE 802.3z 1000BaseLX 标准的 1000BaseLX/LH 接口，但具有较高的光质量，使其在单模光纤（SMF）上的传输距离高达 10km，要比 1000BaseLX 标准中规定的 5km 远一倍。

WS-G5487：WS-5487 遵循 1000BaseZX 标准，工作在普通单模光纤链路上，最大传输距离达 70km，当使用优质单模光纤或散射消除单模光纤时，传输距离可达 100km。WS-G5487 必须与单模光纤一起使用，不能与多模光纤配合使用。由于其收发器具有很强的光质量，因此当使用短距离的单模光纤时，在链路中应该插入一个线上光衰减器以免光接收机过载。防止出现光接收机过载的常见原则如下：

- 只要光纤的长度低于 25km，那么应该在链路两端的光纤和 WS-G5487 的接收端口之间插入一个 10dB 的线上光衰减器。
- 若光纤的长度大于或等于 25km 但低于 50km，那么应该在链路两端的光纤和 WS-G5487 GBIC 的接收端口之间插入一个 5dB 的线上光衰减器。

【问题 3】

该派出所在进行实时调阅时，视频流直接由流媒体服务器转发给解码器进行解码，同时流媒体服务器会复制视频流用于存储，但不会对实时调阅视频流造成延迟，因此整个传输过程为：

模拟信号经编码器进行模数转换为数据帧，经接入、汇聚交换机进行帧转发，经核心交换机模块间转发至流媒体服务器，流媒体服务器处理后，经模块间转发至汇聚派出所流量的汇聚交换机，再经汇聚、接入交换机的帧转发后，至解码器进行数模转换，还原出模拟视频信号播放，则在忽略媒体的信号传输延时的情况下，总延时为：$400+30+30+10+70+10+30+30+400=1010$（ms），不符合规范。

参考答案

【问题 1】

采用“网络节点至监控点直埋光纤”，需要埋设的光缆全部为 2 芯光缆，总长度为 $\sqrt{17}+\sqrt{34}+\sqrt{50}$（km）。

采用“通过光纤汇接点汇接光纤”，需要埋设两种光缆，其中 8 芯光缆总长度为 $\sqrt{18}$ 或 $3\sqrt{2}$，2 芯光缆总长度为 $\sqrt{5}+2\sqrt{2}+2$（km）。

采用“基于 EPON 分光器互连光纤”，需要埋设光缆全部为 2 芯光缆，总长度为 $\sqrt{17}+\sqrt{5}+2$（km）。

【问题 2】

端口 1（至行政区甲）——光电收发器为 WS-G5486，采用高质量单模光纤链路。

端口 2（至行政区乙）——光电收发器为 WS-G5487，采用普通单模光纤链路，但是在光纤和收发器之间必须增加一个 10dB 线上光衰减器。

端口 3（至行政区丙）——光电收发器为 WS-G5487，采用普通单模光纤链路，但是在光纤和收发器之间必须增加一个 5dB 线上光衰减器。

【问题 3】

该派出所在进行实时调阅时，视频流总延时为：400 + 30 + 30 + 10 + 70 + 10 + 30 + 30 + 400 = 1010（ms），大于 1s，不符合规范要求。

可行的优化方案如下：

（1）将接入交换机直接连接至核心交换机，取消汇聚交换机层。

（2）取消接入交换机，直接将编码器、解码器连接至汇聚交换机。

（3）将流媒体服务器的连接端口由服务器连接模块转到汇聚交换机连接模块。

试题二（共 25 分）

阅读以下关于某商贸城企业广域网络升级改造的需求，回答问题 1、问题 2 和问题 3。

某商贸城由商贸城办公主楼、花卉市场、农贸市场、水产品市场、调味品市场和交易中心等几个部分构成，由于各市场覆盖面积较广、用户数量较多、相互间距离较远，因此采用广域网方式建设商贸城的内部企业网络，其网络结构如图 2-1 所示。

商贸城企业网络采用层次化设计，网络节点分为三层：核心层、汇聚层和接入层。核心层由商贸城办公主楼配置 2 台高性能路由器构成，负责与各二级单位路由器进行互联；汇聚层由四个市场的路由器构成，每个市场都是一个网络节点，配置一台路由器，汇聚层与核心层节点间的链路构成主干链路；接入层为各市场的内部局域网络，实现办公人员和商户的接入。

商贸城数据中心业务服务器采用服务器群集技术，服务器都采用双网卡配置，分别对花卉市场、农贸市场、水产品市场、调味品市场提供商贸业务服务。

商贸城企业网的互联网出口部署在商贸城办公主楼，出口带宽为 50Mb/s；商贸城办公主楼至各二级节点之间线路采用“SDH 电路转换为以太网线路”方式，主干链路两端路由器统一采用以太网接口，带宽为 10Mb/s。

随着企业应用发展需要，商贸城决定对企业网络进行升级改造，其建设目标如下：

- 对业务服务器群集网络接入进行改造，使业务压力能均衡分担；
- 将商贸城办公主楼到各个市场网络带宽进行升级；
- 对 Internet 出口带宽进行升级，保证用户能正常上网。

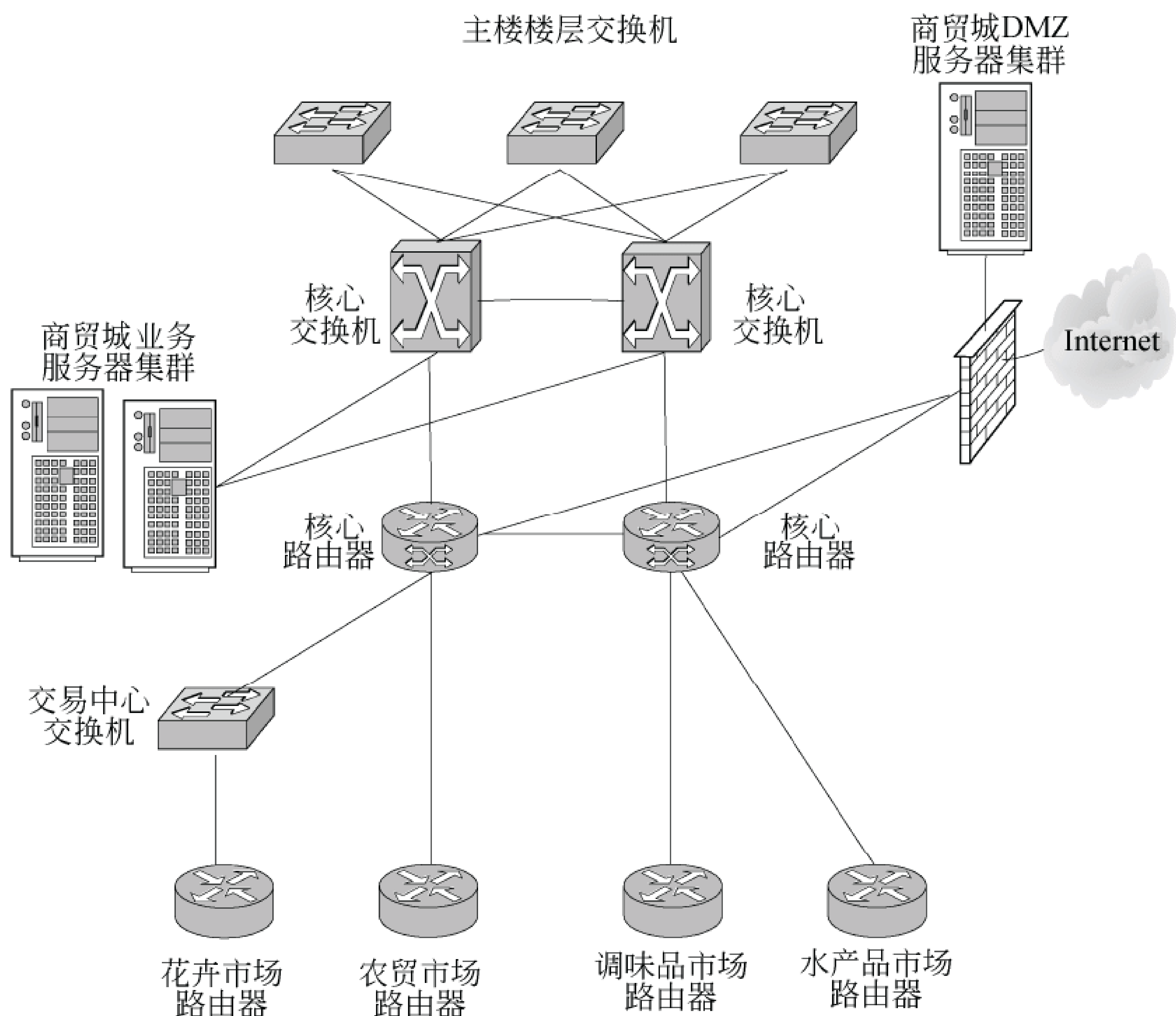


图 2-1　商贸城企业网络示意图

【问题 1】（7 分）

自花卉市场借助于交易中心的局域网交换机接入到企业网络中以来，商户普遍反映访问应用系统和互联网速度较慢，在用户上网高峰时间段，对网络用户的业务开展造成了极大影响。技术人员经过测试发现，从花卉市场路由器 ping 核心路由器延时≥1000ms（其他市场 ping 核心路由器延时≤10ms）。请分析问题出现的原因，并提供可行的解决方案。

【问题 2】（10 分）

为实现各市场和办公主楼之间的线路冗余，决定在各市场路由器至核心路由器之间添加一条冗余线路；在保证线路冗余的同时，为提高主干线路的带宽，需要在主用线路和备用线路之间实现线路的负载均衡。

由于原网络已经采用 OSPF 作为内部网关协议，为减少升级改造工作对路由协议配置的影响，因此决定采用 OSPF 路由负载均衡技术实现对核心层到汇聚层的线路及带宽扩容；而在低链路时期，这种线路扩容方式主要采用多链路 PPP 捆绑技术，请分别叙述采用多链路 PPP 捆绑技术和 OSPF 路由负载均衡技术实现线路及带宽扩容的具体实施步骤。

【问题 3】（8 分）

随着互联网上 P2P、视频点播等类型应用的发展，商户访问互联网行为占据了大量的企业网络带宽，为保证企业内部应用系统的正常服务，提高商户访问互联网和企业应用系统的服务质量，针对该企业网络请给出至少四种优化方法。

试题二分析

本题涉及网络升级改造、性能优化等方面的内容。

【问题 1】

花卉市场作为一个相对独立的专业市场，应该与农贸市场、调味品市场、水产品市场一样，采用路由器之间的点对点链路直接完成互连。

在题设中，花卉市场的路由器并没有与核心路由器之间建立点对点链路，而是借助于交易中心的局域网交换机完成了互连；这就意味着核心路由器的下联端口、花卉市场路由器的上联端口都属于交易中心的局域网络中。

交易中心的局域网络，由交易专用计算机和交换机构成，交易用计算机之间会根据应用需求产生大量的用于二层交换的数据链路层数据帧，同时任何计算机产生的广播报文都会广播至局域网的任何节点，包括核心路由器的下联端口和花卉路由器的上联端口。当交易中心局域网络中计算机数量较多，并且由于应用、病毒等原因，产生大量广播报文或者形成广播风暴时，虽然核心路由器和花卉市场路由器可以屏蔽广播风暴，限制广播报文仅在局域网内传播，但是仍然无法避免核心路由器下联端口和花卉市场上联端口的带宽被广播报文占用，导致路由器之间的实际链路带宽明显下降，这是导致出现花卉市场访问核心网络和其他市场网络效率低下的主要原因。

【问题 2】

多链路 PPP 捆绑技术，部分厂商称为 ML-PPP，即 MultiLink Point-to-Point Protocol；部分厂商称为 PPP-MP，即 Point-to-Point Protocol MultiLink Protocol。是在低链路时期，出于增加带宽的需要，将多个 PPP 链路捆绑使用产生的，简称 MP。MultiLink PPP 允许将报文分片，分片将从多个点对点链路上送到同一个目的地。

在 MP 方式下链路协商过程：

首先和对端进行 LCP 协商，协商过程中，除了协商一般的 LCP 参数外，还验证对端接口是否也工作在 MP 方式下。如果对端不工作在 MP 方式下，则在 LCP 协商成功后，进行一般的 NCP 协商步骤，不进行 MP 捆绑。

然后对 PPP 进行验证，得到对方的用户名。如果在 LCP 协商中得知对端也工作在 MP 方式下，则根据用户名找到为该用户指定的虚拟接口模板，并以该虚拟模板的各项 NCP 参数（如 IP 地址等）为参数进行 NCP 协商，物理接口配置的 NCP 参数不起作用。NCP 协商通过后，即可建立 MP 链路，用更大的带宽传输数据。

使用多链路 PPP 捆绑技术不仅仅可以进行传输带宽扩容，同时可以实现捆绑 PPP 链路之间的负载均衡，这种负载均衡是数据链路层的负载均衡。在实际应用中，多链路 PPP

捆绑的实施需要按照链路扩容、链路捆绑、创建虚拟接口、在虚拟接口上封装 PPP 协议等步骤。

随着以太网络技术的不断成熟，大多数情况下，现有路由器之间的连接主要通过以太网接口实现，在与题设类似的网络升级案例中，主要通过两种方式实现带宽扩容和负载均衡；一种是网络层的负载均衡，主要是通过路由协议的等价路径实现；另一种是数据链路层的负载均衡，主要是通过链路聚合协议，例如 LACP 等；在实际工程领域中，由于链路聚合协议对链路的相同性要求较高，因此使用网络层负载均衡较多。

在多链路的广域网中，如何有效地利用链路，部署流量策略，实现多路径路由选择，一直是网络建设和优化中考虑的重点问题。在静态和动态路由器协议中有效利用链路、部署流量策略的路由技术有很多，包括 ECMP/WCMP、策略路由和多拓扑路由等。其中 ECMP 和 WCMP 是基于目的地的路由，静态路由和 OSPF 支持 ECMP，静态路由、IGRP 和 EIGRP 支持 WCMP；策略路由（Policy-BasedRouting，PBR）是基于 DSCP、端口号、协议等属性静态配置的路径；多拓扑路由（MultiTopologyRouting，MTR）是借助静态和动态路由，依赖网络结构，基于流量类型动态使用多路径到一个给定目的的技术。

ECMP（Equal-CostMultipathRouting，等价多路径）存在多条不同链路到达同一目的地址的网络环境中，如果使用传统的路由技术，发往该目的地址的数据包只能利用其中的一条链路，其他链路处于备份状态或无效状态，并且在动态路由环境下相互的切换需要一定时间，而等值多路径路由协议可以在该网络环境下同时使用多条链路，不仅增加了传输带宽，并且可以无时延无丢包地备份失效链路的数据传输。

ECMP 最大的特点是在实现等值情况下，多路径负载均衡和链路备份的目的，在静态路由和 OSPF 中基本上都支持 ECMP 功能，因此题设中使用 OSPF 协议实现负载均衡和带宽扩容，其关键在于冗余路径的 OSPF COST 值相同。

另外，在大多数厂商的路由器实现时，都存在着两种负载均衡模式，分别是“基于目标网络的负载均衡和快速交换”模式和“基于报文的均分负载和过程交换”模式。

基于目标网络的负载均衡和快速交换：假设到一个网络存在两条路径，那么去往该网络中第一个目标的报文从第一条路径通过，去往网络中的第二个目标的报文从第二条路径走，去往此网络中第三个目标的所有报文还从第一条路径走。路由器工作在默认交换模式下的，即快速交换模式，路由器将使用这种负载均衡方式。

基于报文的均分负载和过程交换：基于报文的均分负载就是第一个去往一个目标网络的报文的链路 1 上发送，下一个去往相同目标网络的报文在另一条链路上发送，对于非等价路径，采用一定比率时报文进行分配。当路由器处于过程交换模式时，将采用基于报文的均分负载方式。

在利用 OSPF 协议实现网络层负载均衡时，需要将路由器由默认的“快速交换”模式切换成“过程交换”模式。

【问题 3】

问题 3 是一个较为典型的案例，网络中存在着多类应用数据流，这些数据流共享网络传输带宽，必然会相互影响。随着应用的不断发展，以及用户对应用带宽及 QoS 的要求不断提升，网络用户会提出应用带宽及 QoS 保障的需求。

对于类似的应用带宽及 QoS 保障需求，主要存在三种优化思路。第一种是扩充整体带宽，通过带宽的扩充，使得所有应用的带宽及 QoS 都得到保障；第二种是在保持带宽不变的基础上，通过添加 QoS 技术，使得应用的带宽及 QoS 得到合理控制，根据应用的重要程度、时段等，保障用户的网络使用满意度；第三种是一种较为根本的做法，也是最彻底的方法，即将网络划分为相对较为独立的业务网络，通过保持网络的单纯性，提升用户的满意度。在实际的工程项目中，可根据用户的网络现状、业务应用分布，采用以上所述三种思路中的一种，或者融合两种以上思路，进行网络优化。

参考答案

【问题 1】

问题出现在交易中心交换机，该交换机既是核心路由器和花卉市场路由器的连接设备，又承担着交易中心客户局域网客户计算机的接入工作，交易中心局域网会产生广播报文，尤其在上网高峰期，大量广播报文形成的广播风暴会占用广域网线路的带宽资源，同时对广域网线路的稳定性造成影响。

可以采用如下的改造方式：改变网络结构，除去核心路由器和交易中心交换机之间的线路，租用新的 SDH 线路，转换为以太网线路后直接连接核心路由器与花卉市场路由器，使得交易中心局域网成为花卉市场路由器下联的一个局域网络。

【问题 2】

多链路 PPP 捆绑技术：

（1）在每个市场的路由器和核心路由器之间扩容一条相同的链路。

（2）通过多链路 PPP 捆绑技术对链路进行捆绑，创建虚拟捆绑接口，并将物理接口添加到虚拟接口的物理接口组中。

（3）在虚拟接口上封装 PPP 协议，并将原有接口的 IP 等信息移植到虚拟接口之上。

（4）保持 OSPF 配置不变，配置完成后可用带宽等于两条链路带宽之和，某一条中断不影响业务的延续性。

OSPF 路由负载均衡技术：

（1）针对每个市场路由器扩容一条相同的链路，但需要连接到另外一台核心路由器。

（2）通过配置上联线路的 cost 值，保证各市场路由器至核心局域网的 metric 值相等。

（3）将各市场路由器的工作模式由快速路由模式（基于目标网络路由模式）修改为过程交换模式（基于报文路由方式）。

（4）OSPF 配置不变，配置完成后实现 IP 包上行时，两条链路的负载均衡，可用带宽等于两条链路带宽之和，某一条链路中断通过 OSPF 协议自动完成路径切换。

【问题 3】

可以采用如下优化方法：

（1）提高商贸城网络主干带宽，使得各市场至办公楼带宽之和远大于互联网出口带宽。

（2）增加目前因特网出口总带宽，限制单个用户访问因特网流量，给企业业务应用预留带宽。

（3）在互联网出口处添加流量控制设备，在高峰时段限制 P2P、视频点播等大流量应用，在非高峰时段则不限制应用流量。

（4）启用 DiffServ 技术，基于主干路由器设备划分 DiffServ 域，并针对企业业务和互联网业务形成不同业务级别，提供不同的服务质量。

（5）增加第二运营商线路和流量负载均衡设备实现基于目的地址和业务类型的智能流量负载均衡及带宽保障。

（6）建立多因特网出口，实现业务因特网出口与因特网上网出口分离互不影响，从而从资源上和稳定性上最大程度地保障业务应用。

（7）对现有网络进行改造，建立业务网络和互联网隔离制度，对商户同时提供业务网络与互联网络接入，保证两类业务相互不受影响。

试题三（25 分）

阅读以下关于某市行政审批服务中心网络规划的叙述，回答问题 1、问题 2 和问题 3。

某市行政审批服务中心大楼内涉及几类网络：互联网 Internet、市电子政务专网、市电子政务外网、市行政审批服务中心大楼内局域网以及各部门业务专网。行政审批服务中心网络规划工作组计划以市电子政务专网为基础，建设市级行政审批服务中心专网（骨干万兆、桌面千兆）。大楼内部署五套独立链路，分别用于连接政务外网、政务专网、大楼内局域网、互联网和涉密部门内网。行政审批服务中心网络结构（部分）如图 3-1 所示。

【问题 1】（6 分）

请指出图 3-1 的安全接入平台中可采用的技术或安全设备有哪些？

【问题 2】（4 分）

图 3-1 中 DMZ 区交换机共提供 12 个千兆端口和 8 个百兆端口，请问该交换机的吞吐量至少达到多少 Mpps，才能够确保所有端口均能线速工作，并提供无阻塞的数据交换。

【问题 3】（15 分）

市行政审批服务中心大楼监控系统采用目前国际上最先进的 IP 智能监控架构，并且能和门禁系统、报警系统、车牌管理系统进行联动。大楼监控系统可提供实时监控、存储和随时调看 CIF 格式（352×288）和 D1 格式（720×576）分辨率的图像，支持 MPEG2、

MPEG4、H.264 等编码格式，尤其是在高动态图像监控场合，可以提供广播级的高清图像质量，满足市大楼安防监控的要求。

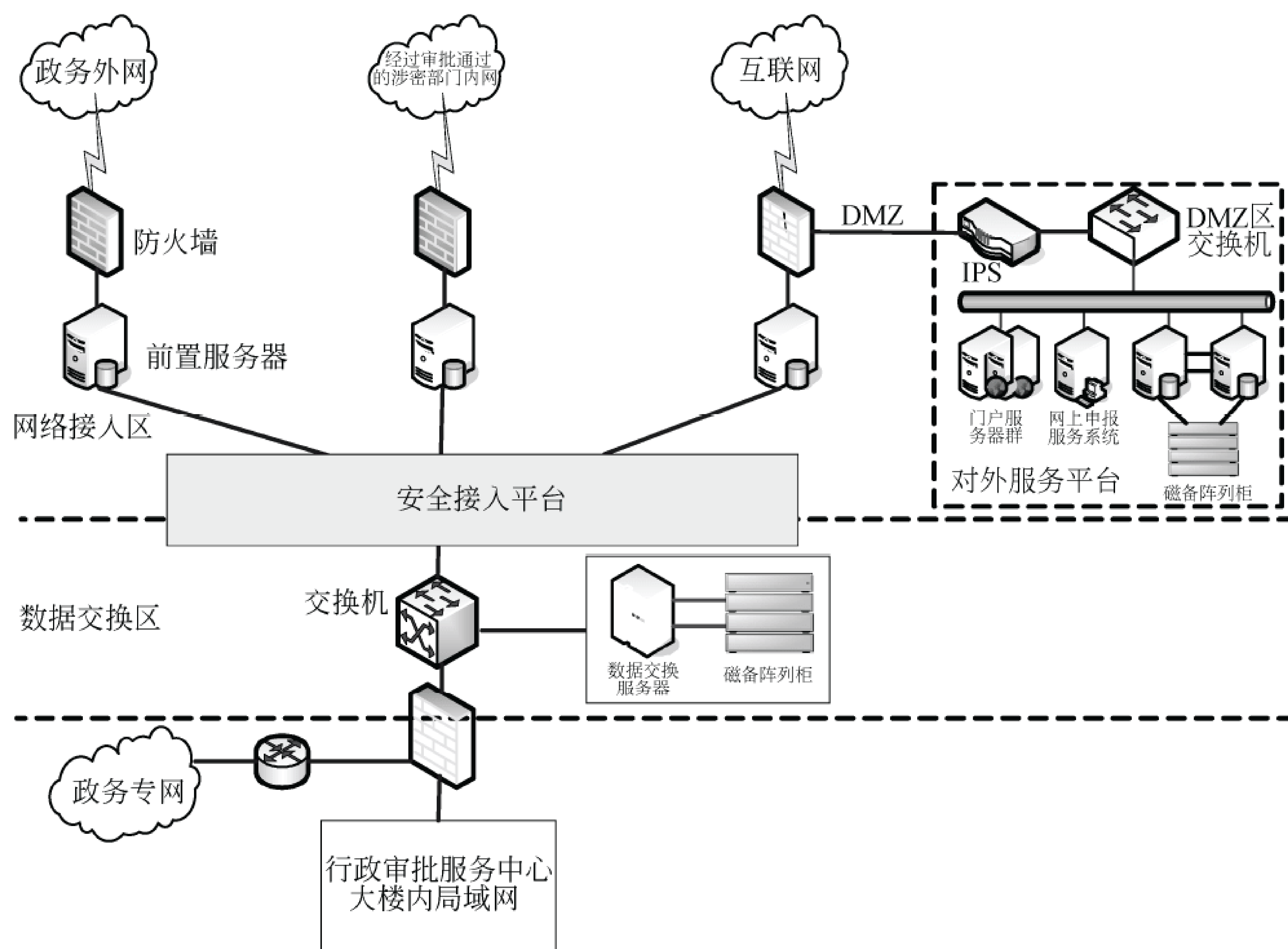


图 3-1　行政审批服务中心部分网络结构图

（1）大楼内预计共有监控点 500 个，如果保存的是 CIF 格式的图像，码流为 512Kb/s，请计算每小时保存楼内全部监控点视频流需要多大的存储空间（Bytes 或 GB）。

如果保存的是 D1 格式的图像，码流为 2048Kb/s，请计算每小时保存楼内全部监控点视频流需要多大的存储空间（Bytes 或 GB）。

（2）系统实施时，图像格式采用了 CIF，码流为 512Kb/s，请计算保存楼内全部监控点 30 天视频流需要的存储空间（Bytes、GB 或 TB）。

全部监控视频流信息保存在 IPSAN 设备 S2600 中（S2600 控制框：双控，220v 交流，4GB 内存，8*GE iSCSI 主机接口，磁盘数量 12 个/框，最大支持附加 7 个磁盘扩展框）。假设在本项目中采用 SATA 1TB 7.2K RPM 硬盘，在 IPSAN 配置的 RAID 组级别为 RAID10。

请指出 RAID10 的磁盘利用率，并计算出保存 30 天视频流至少需要的硬盘数，以及至少需要配置的 S2600 控制框数量。

（3）假设在 IPSAN 设备中创建了 2 个 RAID 组 RAID001 和 RAID002，其中 RAID001

组采用 RAID5，包含 6 个磁盘，RAID002 组采用 RAID6，包含 8 个磁盘。请分别计算这两个 RAID 组的磁盘利用率。

试题三分析

本题考查的是安全接入平台的架构及网络存储设备的相关知识。

【问题 1】

本问题考查的是安全接入平台的架构方法，即可采用哪些安全技术或安全设备来架构安全接入平台。根据题目要求，安全接入平台较常见的技术或设备包括：通过防火墙建立隔离本地和外部网络的防御系统；通过 IDS/IPS 监视经过防火墙的全部通信并且查找可能是恶意的攻击通信，并在这种攻击扩散到网络的其他地方之前阻止这些恶意的通信；通过部署身份认证服务器来组织管理个人身份认证信息；利用可信边界安全网关保证用户的物理身份与数字身份相符；通过 CA 服务器对数字证书进行发放和管理；利用 IPSec VPN 实现多专用网安全连接；通过集中监控审计对网络中的各种设备和系统进行集中的、可视的综合审计，及时发现安全隐患，提高安全系统成效；利用网闸从物理上隔离、阻断了具有潜在攻击可能的连接，从根本上杜绝可被黑客利用的安全漏洞。

【问题 2】

本问题考查的是交换机线速工作并提供无阻塞的数据交换的衡量标准。包转发线速的衡量标准是以单位时间内发送 64B 的数据包（最小包）的个数作为计算基准的。对于千兆以太网来说，计算方法如下：1 000 000 000bps/8bit/（64+8+12）B=1 488 095pps。说明：当以太网帧为 64B 时，需考虑 8B 的帧头和 12B 的帧间隙的固定开销。故一个线速的千兆以太网端口在转发 64B 包时的包转发率为 1.488Mpps。快速以太网的端口包转发率正好为千兆以太网的十分之一，为 0.1488Mpps。而满配置吞吐量（Mpps）=千兆端口数量×1.488 Mpps+百兆端口数量×0.1488Mpps+其余类型端口数。

根据题目要求，满配置吞吐量（Mpps）=12×1.488Mpps+8×0.1488Mpps= 17.856+1.1904= 19.0464Mpps，因此该交换机吞吐量必须大于 19.0464Mpps，才认为该交换机采用的是无阻塞的结构设计。

【问题 3】

本问题考查的是网络存储设备在保存不同格式文件时存储容量的计算。

（1）CIF 为常用视频标准化格式（Common Intermediate Format）的简称。在 H.323 协议簇中，规定了视频采集设备的标准采集分辨率，CIF 的标准采集分辨率为 352×288 像素。D1 是数字电视系统显示格式的标准，标准采集分辨率为 720×480 像素。

根据题目要求，由于 CIF 格式的图像码流为 512Kb/s，先计算保存每个监控点每秒图像需要的存储空间：即将 512Kb 转化为 512×1024/8B，再乘以监控时间 3600s（1 小时）和监控点的数量 500，即得到最后的结果：

$$512\times1024/8\times3600\times500=112\ 500\text{MB}\approx109.86\text{GB}$$

如果保存的是 D1 格式的图像，除了码流为 2 048Kb/s 与上述不同外，其余计算方法完全相同：

$$2048\times1024/8\times3600\times500=450\ 000\text{MB}\approx439.45\text{GB}$$

（2）如果保存的是 CIF 格式的图像，码流为 512Kb/s，保存楼内全部监控点 30 天视频流需要的存储空间计算方法和（1）类似，只要再乘上 24 小时和 30 天即可：

$$512\times1024/8\times3600\times500\times24\times30=81\ 000\ 000\text{MB}\approx79\ 101.56\text{GB}\approx77.25\text{TB}$$

RAID 10 将数据分散存储到 RAID 组的成员盘上，同时为每个成员盘提供镜像盘，实现数据全冗余保存。RAID 10 的磁盘利用率为 1/*m*（*m* 为镜像组内成员盘个数）。根据题意，要计算出保存 30 天视频流至少需要的硬盘数，即要使 RAID 10 的磁盘利用率最大，因此取 *m*=2，RAID 10 最大的磁盘利用率为 1/2×100%=50%。根据上面计算出来的保存楼内全部监控点 30 天视频流需要的存储空间，可得本项目需要 77.25TB×2=154.5TB 的存储空间，由于所采用的是 1TB 的硬盘，因此保存 30 天视频流至少需要 155 块硬盘。

每个 S2600 控制框加上扩展框满配时可以支持 12×8=96 块硬盘，因此本项目需要 2 个控制框。

（3）RAID 5 为保障存储数据的可靠性，采用循环冗余校验方式，并将校验数据分散存储在 RAID 组的各成员盘上，RAID 5 允许 RAID 组内一个成员盘发生故障。当 RAID 组的某个成员盘出现故障时，通过其他成员盘上的数据可以重新构建故障磁盘上的数据。RAID 5 磁盘利用率为（*n*–1）/*n*（*n* 为 RAID 组内成员盘个数），当 RAID 组由 3 个磁盘组成时，利用率最低，为 66.7%。RAID001 组采用 RAID 5，包含 6 个磁盘，其硬盘利用率=（6–1）/6×100%=83.33%。

RAID 6 对数据进行两个独立的逻辑运算，得出两组校验数据。同时将这些校验数据分布在 RAID 组的各成员盘上。RAID 6 允许 RAID 组内同时有两个成员盘发生故障。故障盘上的数据可以通过其他成员盘上的数据重构。RAID 6 磁盘利用率为（*n*–2）/*n*（*n* 为 RAID 组内成员盘个数），当 RAID 组由 4 个磁盘组成时，利用率最低，只有 50%。RAID002 组采用 RAID 6，包含 8 个磁盘，其硬盘利用率=（8–2）/8×100%=75%。

参考答案

【问题 1】

安全接入平台可采用的技术或设备包括：可信边界安全网关、IPSec VPN、防火墙、身份认证服务器、IDS/IPS、集中监控审计、网闸、CA 服务器等设备。

【问题 2】

满配置吞吐量（Mpps）=12×1.488Mpps+8×0.1488Mpps=17.856+1.1904=19.0464 Mpps，因此该交换机吞吐量必须大于 19.0464Mpps，才认为该交换机采用的是无阻塞的结构设计。

【问题 3】

（1）如果保存的是 CIF 格式的图像，码流为 512Kbps，每小时保存楼内全部监控点视频流需要的存储空间是：

$$512\times1024/8\times3600\times500=112\,500\text{MB}\approx109.86\text{GB}$$

如果保存的是 D1 格式的图像，码流为 2048Kbps，每小时保存楼内全部监控点视频流需要的存储空间是：

$$2048\times1024/8\times3600\times500=450\,000\text{MB}\approx439.45\text{GB}$$

（2）如果保存的是 CIF 格式的图像，码流为 512Kbps，保存楼内全部监控点 30 天视频流需要的存储空间是：

$$512\times1024/8\times3600\times500\times24\times30=81\,000\,000\text{MB}\approx79\,101.56\text{GB}\approx77.25\text{TB}$$

RAID 10 最大的硬盘利用率为 1/2×100%=50%，因此本项目需要 77.25TB×2=154.5TB，所以保存 30 天视频流至少需要 155 块硬盘。

每个 S2600 控制框加上扩展框满配时可以支持 96 块硬盘，因此本项目需要 2 个控制框。

（3）RAID001 组采用 RAID5，包含 6 个磁盘，其硬盘利用率=（6–1）/6×100%=83.33%。

RAID002 组采用 RAID6，包含 8 个磁盘，其硬盘利用率=（8–2）/8×100%=75%。

第 6 章　2010 上半年网络规划设计师下午试卷 II 写作要点

试题一　论网络规划与设计中的可扩展性问题

网络技术的发展非常迅速，不仅原有技术不断升级换代，而且新的技术也不断涌现。同时，组织的网络应用需求也在不断提升，这一切对网络的升级提出了迫切需求。而组织的网络经常重建的可能性非常小，一般都是采取升级的方式来提高网络的性能。这就要求网络在规划和设计之初要充分考虑网络的可扩展性。

请围绕“网络规划与设计中的可扩展性问题”论题，依次对以下三个方面进行论述。

1．简要叙述你参与设计和实施的大中型网络项目以及你所担任的主要工作。

2．详细论述你在网络规划和设计中提高网络可扩展性的思路与策略，以及所采用的技术和方法。

3．分析和评估你所采用的提高网络可扩展性措施的效果，以及相关的改进措施。

写作要点

1．叙述自己参与设计和实施的网络项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量。

2．能够全面和深入地论述提高网络可扩展性的思路与策略以及所使用的技术和方法，从硬件、软件以及管理措施等多个角度进行说明，具有一定的广度和深度。主要从以下几个方面进行论述：

（1）在网络拓扑结构方面

（2）在综合布线方面

（3）在网络设备方面

（4）在系统软件、应用软件方面

（5）在网络管理方面

（6）在网络安全方面

3．对提高网络可扩展性措施的效果以及需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

试题二　论大中型网络的逻辑网络设计

逻辑网络设计是网络规划与设计中的关键阶段。逻辑网络设计和规划的目标包括合理的网络结构、成熟而稳定的技术选型、合适的运营成本以及使逻辑网络具备可扩充、易用、可管理和安全等性能。

请围绕“大中型网络的逻辑网络设计”论题，依次对以下三个方面进行论述。

1．简要叙述你参与设计和实施的大中型网络项目以及你所担任的主要工作。

2．针对大中型网络中逻辑网络设计的主要工作内容论述你是如何进行逻辑网络设计的。

3．简要介绍你在大中型网络的逻辑网络设计中遇到的棘手问题及其解决办法。

写作要点

1．叙述自己参与设计和实施的网络项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量。

2．能够全面和深入地阐述大中型网络的逻辑网络设计的主要工作内容、采用了哪些技术和方法，这些技术和方法要针对大中型网络的特点，具有一定的广度和深度。主要应包括以下内容：

（1）网络结构的设计

（2）物理层技术选择

（3）局域网、广域网技术选择

（4）地址和命名模型设计

（5）交换和路由协议的选择

（6）网络安全策略设计

（7）网络管理策略设计

3．在大中型网络的逻辑网络设计中遇到的问题及其解决办法，应有具体的着眼点，不能泛泛而谈。

第 7 章　2010 下半年网络规划设计师上午试题分析与解答

试题（1）

TDM 和 FDM 是实现多路复用的基本技术，有关两种技术叙述正确的是__（1）__。

（1）A. TDM 和 FDM 都既可用于数字传输，也可用于模拟传输

B. TDM 只能用于模拟传输，FDM 只能用于数字传输

C. TDM 更浪费介质带宽，FDM 可更有效利用介质带宽

D. TDM 可增大通信容量，FDM 不能增大通信容量

试题（1）分析

本题考查时分多路复用（TDM）和频分多路复用（FDM）的基础知识。

TDM（Time-Division Multiplexing）方法的原理是把时间分成小的时隙（Time slot），每一时隙由一路信号占用，每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙，每个用户所占用的时隙周期性地出现。显然，时分复用的所有用户在不同的时间占用全部的频带带宽。在进行通信时，复用器和分用器总是成对地使用，在复用器和分用器之间是用户共享的高速信道。如果一个用户在给定的时隙没有数据传送，该时隙就空闲，其他用户也不能使用，因为时隙的分配是事先确定的，接收方根据事先分配的时间确定在哪个时隙接收属于自己的数据。TDM 用于数字传输。

FDM（Frequency-Division Multiplexing）的基本原理是将多路信号混合后放在同一传输介质上传输。多路复用器接收来自多个数据源的模拟信号，每个信号有自己独立的频带。这些信号被组合成另一个具有更大带宽、更加复杂的信号，合成的信号被传送到目的地，由另一个多路复用器完成分解工作，把各路信号分离出来。FDM 用于模拟传输。

参考答案

（1）C

试题（2）、（3）

带宽为 3KHz 的信道，在无噪声条件下传输二进制信号的极限数据率和在信噪比为 30dB 条件下的极限数据率分别为__（2）__。该结果说明__（3）__。

（2）A. 6Kbps，30Kbps　　B. 30Kbps，6Kbps

C. 3Kbps，30Kbps　　D. 3Kbps，3Kbps

（3）A. 结果一样　　B. 有噪声时结果更好

C. 无噪声时结果更好　　D. 条件不同不可比

试题（2）、（3）分析

本题考查有关带宽与数据率的关系及数据率计算方法的基础知识。其计算方法为：

对没有噪声的信道，利用奈奎斯特准则计算信道的极限数据率，该准则为：在带宽为 W（Hz）的无噪声信道上传输信号，假定每个信号取 V 个离散电平值，则信道的极限数据率（比特率）为

$$2W*\log_2 V \text{（bps）}$$

对有噪声的信道，利用香农定理计算信道的极限数据率，该定理为：在带宽为 W（Hz）的有噪声信道上传输信号，假定信噪比为 S/N（功率比），则信道的极限数据率为

$$W*\log_2(1+S/N) \text{（bps）}$$

上述两个计算公式的条件是不一样的。对奈奎斯特准则，考虑每个信号可表示的状态数是 V，其特例是 $V=2$，即每个信号可表示两个状态之一（0 或 1）。而香农定理不限制每个信号表示的状态数。

参考答案

（2）A　　（3）D

试题（4）

传输介质越长，传播延迟越大，由此导致的延迟失真越大。受延迟失真影响最大的是__（4）__。

（4）A. 低速、数字信号　　B. 高速、数字信号
C. 低速、模拟信号　　D. 高速、模拟信号

试题（4）分析

本题考查传输损害方面的基础知识。

延迟失真是有线传输介质独有的现象，这种变形是由有线介质上信号传播速率随着频率而变化所引起的。在一个有限的信号频带中，中心频率附近的信号速度最高，而频带两边的信号速度较低，这样，信号的各种频率成分将在不同的时间到达接收器。

延迟失真对数字信号影响尤其重大，一个位元的信号成分可能溢出到其他的位元，引起信号内部的相互串扰，这将限制传输的位速率。

参考答案

（4）B

试题（5）、（6）

当千兆以太网使用 UTP 作为传输介质时，限制单根电缆的长度不超过__（5）__米，其原因是__（6）__。

（5）A. 100　　B. 925　　C. 2500　　D. 40000

（6）A. 信号衰减严重　　B. 编码方式限制
C. 与百兆以太网兼容　　D. 采用 CSMA/CD

试题（5）、（6）分析

本题考查以太网的基本原理。

传统以太网采用 CSMA/CD 访问控制方式，规定单根 UTP 电缆的长度不超过 100m，

最大介质长度以及最小帧长度的确定原则是：能确保一个帧在发送过程中若出现冲突，则一定能够发现该冲突。发展到千兆以太网，虽然数据率提高，但访问方式（帧的发送与接收方式）、帧的格式、介质长度维持不变，以保持与传统以太网的兼容。

介质的最长长度确定了时间片（信号在介质上往返传输的时间）的长度：假定节点 A、B 分别在总线的两端，A 首先向 B 发送信息。假定 A 发送的信息即将到达 B 时，B 开始向 A 发送信息，此时 B 没有检测到冲突，但刚刚开始发送后 A 的信息到达，B 检测到了冲突。B 发送的信息到达 A 后，A 检测到了冲突。从这一过程，我们可以得出下述结论：

（1）为确保一个节点（如 A）在任何时候都能够检测到可能发生的冲突，需要的时间是信号在总线上往返传输的时间，此时间被称为时间片，也称为冲突域、冲突窗口、争用期，而这个时间是由介质的长度决定的。

（2）为保证在冲突发生后能够检测到冲突，必须保证在冲突发生并被检测到时，帧本身没有发送完（因为发送完后即使出现了冲突也不检测），因此需要为帧设定一个最短长度。

（3）争用期、最短帧长度确定了，介质的最大长度也就确定了。这也是为什么局域网的介质长度都受到严格限制，而广域网的长度无此限制的原因。

参考答案

（5）A　　（6）D

试题（7）、（8）

对无线局域网，可显著提高数据率的技术是__（7）__。对有 2 台计算机、1 个 AP、采用 300Mbps 的 802.11n 的 WLAN，2 台计算机数据传输的概率相同，则每台计算机实际传送用户数据的最大理论速度最接近__（8）__MB/s。

（7）A. CSMA/CA　　B. CSMA/CD　　C. CDMA　　D. MIMO

（8）A. 1.4　　B. 6.7　　C. 9.3　　D. 18.7

试题（7）、（8）分析

本题考查的是无线局域网（WLAN）的基本知识。

WLAN 采用 CSMA/CA 访问控制方式，多台计算机竞争使用一个信道与 AP 通信以发送数据，计算机越多，冲突的机会越多，每台计算机实际获得的发送数据的机会越少，这种方式限制了一个 AP 可服务的计算机的数量即网络的规模。

MIMO 方式利用多个天线，分别使用不同的信道（频率），可同时传输更多的信号，使得一台计算机与 AP 之间的数据率显著提高，也允许更多的计算机同时传输数据。

对于 2 台计算机、1 个 AP 的情况，因发送概率相同，则每台计算获得的实际数据率可认为是总带宽的一半即 150Mbps，换算成以字节为单位的数据率 18.75MB/s。

此题可进一步精确：WLAN 帧最大长度为 2346B，其中数据部分最大长度为 2312B，所以每台计算机实际发送用户数据的最大理论速度的近似值可表示为 18.75MB/s

*2312/2346≈18.5MB/s。

参考答案

（7）D （8）C

试题（9）

阻塞包算法（反馈抑制法）是一类典型的基于闭环控制原理的拥塞控制方法，其主要缺点之一是__（9）__。

（9）A. 显著降低通信效率 B. 可能导致不公平

C. 不能真正控制拥塞 D. 降低网络可用性

试题（9）分析

本题考查拥塞控制方面的基本知识。

阻塞包算法是利用闭环原理实现拥塞控制的一种方案，其目标是在拥塞发生时起作用，而在没有拥塞时不起作用，以最大限度地提高系统的吞吐量和效率。

阻塞包算法假设每条输出线有两个变量 μ 和 f，μ 为近期利用率，其值为 $0\leqslant\mu\leqslant 1$，f 为瞬时利用率，其值为 0 或 1。定义公式 $\mu_{新}=\alpha\mu_{旧}+(1-\alpha)f$，$\alpha$ 取 0～1 之间的数值，反映输出线利用率修改的周期。可为 μ 定义一个阈值，当 μ 大于此值时，进入报警状态，否则算法不起作用。

阻塞包算法的工作过程可描述为：

①（测量）节点收到包，重新计算 μ 值。

②（判断）根据 μ 值判断是否为报警状态?

若不是，则转发包，转①处理下一个包。

若是，则转③。

③（报警）判断该包在其他节点上是否触发发送过阻塞包？

若没有，则向源节点发送一个阻塞包，同时在收到的数据包上填入已发阻塞包标志。

转发包，转①。

④（抑制）源节点在收到阻塞包后，将发送包的速度降低 X%。当在规定的时间间隔 τ 内如果没有收到新的阻塞包，就将发送速度提高 Y%($Y<X$)。

该算法的缺点之一是可能导致不公平。源端主机在收到阻塞包后需要降低发送速度，但是可能会因某种原因导致多个数据源收到阻塞包的时间上有差异，使得有些源端因发送速度快已发送完而没有降低发送速度，有些源端因发送速度慢或数据多没有发送完而降低了发送速度，从而可能造成一种“慢的更慢”的情况，这对各主机来说是不公平的。

参考答案

（9）B

试题（10）

距离向量路由算法要求每个节点保存一张距离向量表（即路由表），其中最关键的

路由信息是__（10）__。

（10）A. 源节点到目的节点的最短距离
B. 源节点到目的节点的路径
C. 本节点到目的节点的输出节点（下一节点）地址
D. 本节点到目的节点的路径

试题（10）分析

本题考查路由算法与协议方面的基本知识。

距离向量路由算法要求每个节点保存一张距离向量表（即路由表），其中包括各目的节点、本节点到对应目的节点的最短距离、本节点到目的节点的输出节点（下一节点）地址。

参考答案

（10）C

试题（11）

SDH 网络是一种重要的广域网，具有多种网络结构，可简述为__（11）__。

（11）A. 星型网结构借助 TM 设备连接，主要用作专网
B. 链型网结构借助 DXC 设备连接，主要用作接入网
C. 环型网结构借助 ADM 设备连接，主要用作骨干网
D. 网孔型结构借助 ADM 设备连接，主要用作长途骨干网

试题（11）分析

本题考查 SDH 网络的基本知识。

SDH 网络是一种重要的广域网，具有多种网络结构，主要有：利用 ADM 连接的链型网、利用 DXC/ADM 连接的星型网、利用 DXC/ADM 连接的树型网、利用 ADM 连接的环型网、利用 DXC/ADM 连接的网孔型网。

SDH 网络主要用作骨干网，用于连接本地网。

参考答案

（11）C

试题（12）

EPON 是一种重要的接入技术，其信号传输模式可概括为__（12）__。

（12）A. 采用广播模式，上下行均为 CSMA/CD 方式
B. 采用点到多点模式，下行为广播方式，上行为 TDMA 方式
C. 采用点到点模式，上下行均为 WDM 方式
D. 采用点到点模式，上下行均为 CSMA/CD 方式

试题（12）分析

本题考查接入网中 EPON 网的基本知识。

EPON 是第一英里以太网联盟（EFMA）在 2001 年初提出的基于以太网的无源光接

入技术，IEEE 802.3ah 工作小组对其进行了标准化，EPON 可以支持 1.25Gbps 对称速率，未来可升级到 10 Gbps。EPON 由于其将以太网技术与 PON 技术完美结合，因此非常适合 IP 业务的宽带接入。Gbps 速率的 EPON 系统也常被称为 GE-PON。

EPON 的主要特点有：

- 采用 P2MP（点到多点）传输
- 单纤双向
- 树型结构，ODN 可级联
- 信号：下行—广播；上行—TDMA；到达 OLT，不会到达其他的 ONU
- 波长：下行—1550nm，上行—1310nm，采用 WDM 方式传输
- 速率：1Gbps（未来 10Gbps）

参考答案

（12）B

试题（13）、（14）

甲机构构建网络时拟采用 CIDR 地址格式，其地址分配模式是 210.1.1.0/24，则实际允许的主机数最大为__（13）__。如果乙机构采用的地址分配模式是 210.1.0.0/16，对于目的地址为 210.1.1.10 的数据分组，将被转发到的位置是__（14）__。

（13）A. 2^{24}　　B. 2^{8}　　C. $2^{24}-2$　　D. $2^{8}-2$

（14）A. 甲机构的网络　　B. 乙机构的网络

C. 不确定　　D. 甲、乙之外的一个网络

试题（13）、（14）分析

本题考查 IP 地址，特别是 CIDR 地址格式的基本知识。

CIDR（Classless Inter-Domain Routing）将 IP 地址看成两级结构，用“IP 首地址/网络前缀位数”的形式表示。在一个网络内表示主机的地址位数为 32-网络前缀位数。全 0 和全 1 的地址不能作为普通地址分配。

对于 CIDR 格式的 IP 地址，在进行路由选择时遵循的原则是最长匹配，即选择路由表中网络前缀部分与分组中 IP 地址前缀部分的相同部分最长的那个地址作为转发地址。

参考答案

（13）D　　（14）A

试题（15）

IPv6 地址分为 3 级，其中第 1 级表示的含义是__（15）__。

（15）A. 全球共知的公共拓扑　　B. 本地网络　　C. 网络接口　　D. 保留

试题（15）分析

本题考查 IPv6 的基本内容。

IPv6 地址通常分为 3 级，第一级为公共拓扑，表示多个 ISP 的集合；第二级为站点拓扑，表示一个机构内部子网的层次结构；第三级唯一标识一个接口。

参考答案

（15）A

试题（16）

关于 ARP 协议，描述正确的是＿（16）＿。

（16）A. 源主机广播一个包含 MAC 地址的报文，对应主机回送 IP 地址
B. 源主机广播一个包含 IP 地址的报文，对应主机回送 MAC 地址
C. 源主机发送一个包含 MAC 地址的报文，ARP 服务器回送 IP 地址
D. 源主机发送一个包含 IP 地址的报文，ARP 服务器回送 MAC 地址

试题（16）分析

本题考查 ARP 协议的基本内容。

ARP 协议的功能是通过已知的 IP 地址找到对应的 MAC 地址，其基本方法是：当需要获取 MAC 地址时，就广播一个包含 IP 地址的消息，收到该消息的每台计算机根据自己的 IP 地址确定是否应答该消息。若是被询问的机器，则发送一个应答消息，将自己的 MAC 地址置于其中，否则不作应答。每个机器就只需记住自身的 IP 地址，且该地址可动态改变。

参考答案

（16）B

试题（17）

RIP 协议根据从邻居节点收到的路由信息更新自身的路由表，其更新算法的一个重要步骤是将收到的路由信息中的距离改为＿（17）＿。

（17）A. ∞　　B. 0　　C. 15　　D. 原值加 1

试题（17）分析

本题考查有关 RIP 协议的基本知识。

RIP 协议更新路由的算法如下：

（1）收到相邻路由器 X 的 RIP 报文，为方便，将其称为路由表 X（一个临时表）。将路由表 X 中“下一跳路由器地址”字段都改为 X，将所有“距离”都加 1（含义是：假定本路由器的下一跳为 X，原来从 X 到达的网络的距离加上从本路由器到 X 的距离）；

（2）对修改后的路由表 X 的每一行，重复：

若目的网络不在本地路由表中，则将该行添加到本地路由表中；

否则，若下一跳的内容与本地路由表中的相同，则替换本地路由表中的对应行；

否则，若该行的“距离”小于本地路由表中相应行的“距离”，则用该行更新本地路由表中的相应行；

否则，返回。

（3）若 180 秒未收到邻居 X 的路由表，则将到邻居路由器 X 的距离置为 16。

参考答案

（17）D

试题（18）、（19）

TCP 协议在工作过程中存在死锁的可能，其发生的原因是 （18） ，解决方法是 （19） 。

（18）A. 多个进程请求未被释放的资源
B. 一个连接还未释放，又请求新的连接
C. 接收方发送 0 窗口的应答报文后，所发送的非 0 窗口应答报文丢失
D. 定义 RTT 值为 2 倍的测量值不恰当

（19）A. 禁止请求未被释放的资源
B. 在一个连接释放之前，不允许建立新的连接
C. 修改 RTT 的计算公式
D. 设置计时器，计时满后发探测报文

试题（18）、（19）分析

本题考查 TCP 协议的基本知识。

TCP 协议在工作过程中可能发送死锁的原因是：接收方为暂缓接收数据而向发送方发送窗口为 0 的应答报文，发送方收到后暂停发送，等待接收到非 0 窗口的应答报文后继续发送新的报文。如果接收方在发送 0 窗口的应答报文后，所发送的非 0 窗口应答报文丢失，则发送方会一直等待下去。解决这一问题的方法是：发送方设置计时器，在收到 0 窗口应答报文后启动计时，计时满后向接收方发探测报文，提醒接收方重发非 0 窗口的应答报文。

参考答案

（18）C （19）D

试题（20）

FTP 需要建立两个连接，当工作于 Passive 模式时，其数据连接的端口号是 （20） 。

（20）A. 20 B. 21
C. 由用户确定的一个整数 D. 由服务器确定的一个整数

试题（20）分析

本题考查 FTP 协议的基本知识。

FTP 支持两种模式，一种叫做 Standard（也就是 PORT 方式，主动方式），另一种叫 Passive（也就是 PASV，被动方式）。

（1）Standard 模式（PORT 模式）

Standard 模式是 FTP 的客户端发送 PORT 命令到 FTP 服务器。FTP 客户端首先和 FTP 服务器的 TCP 21 端口建立连接，通过这个连接发送命令，客户端需要接收数据的时候在这个连接上发送 PORT 命令，其中包含了客户端用于接收数据的端口。服务器端通过自己的 TCP 20 端口连接至客户端指定的端口建立数据连接发送数据。

（2）Passive 模式（PASV 模式）

Passive 模式是 FTP 的客户端发送 PASV 命令到 FTP 服务器。在建立控制连接的时候和 Standard 模式类似，但建立连接后发送的不是 PORT 命令，而是 PASV 命令。FTP 服务器收到 PASV 命令后，随机打开一个高端端口（端口号大于 1024）并且通知客户端在这个端口上传送数据，客户端连接 FTP 服务器此端口（非 20）建立数据连接进行数据的传送。

参考答案

（20）D

试题（21）

DNS 通常会为域名设定一个有效期（时间长度）。如果要使域名永久有效，则有效期的值应设为＿（21）＿。

（21）A. 0　　B. 65535　　C. 86400　　D. 4294967295（即 $2^{32}-1$）

试题（21）分析

本题考查 DNS 的基本知识。

DNS 规定，域名的有效时间以秒为单位，用 86400 秒（24 小时）表示永久有效。

参考答案

（21）C

试题（22）

使用 SMTP 协议发送邮件时，当发送程序（用户代理）报告发送成功时，表明邮件已经被发送到＿（22）＿。

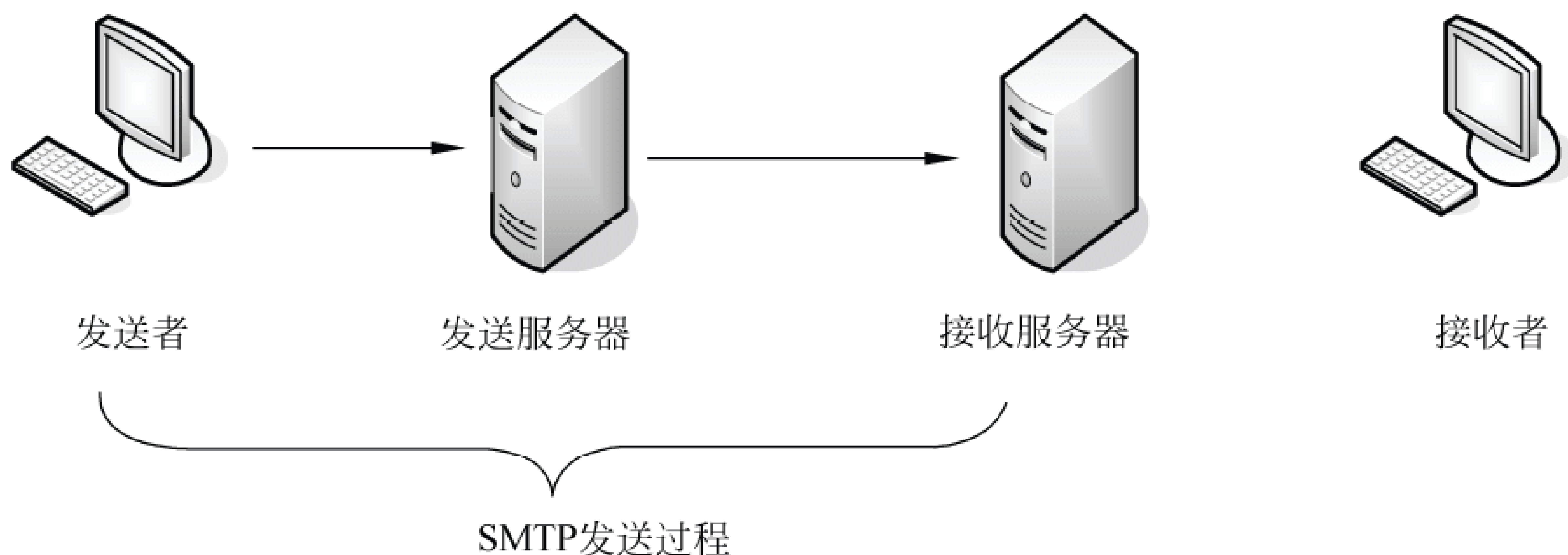
（22）A. 发送服务器上　　B. 接收服务器上

C. 接收者主机上　　D. 接收服务器和接收者主机上

试题（22）分析

本题考查 SMTP 协议的基本知识。

SMTP 的发送过程如下图所示，分两个阶段完成。发送程序（用户代理）只负责从用户计算机到发送服务器之间的发送。



参考答案

（22）A

试题（23）、（24）

MIB 中的信息用 TLV 形式表示。二进制位串“110”用 TLV 形式表示时，实际占用的字节数是＿（23）＿。TLV 形式的数据被 SNMP 协议传输时，被封装成＿（24）＿进行传输。

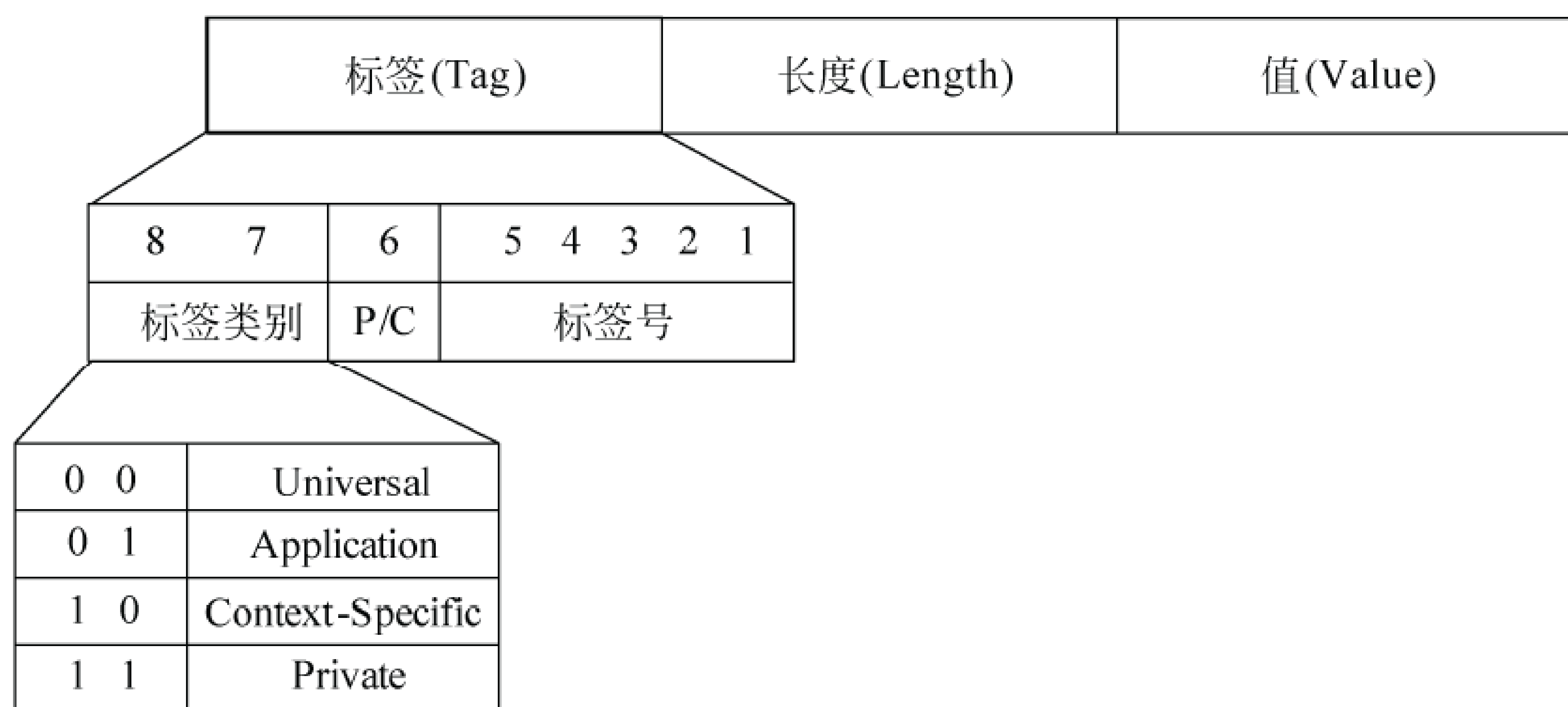
（23）A. 1　　B. 2　　C. 3　　D. 4

（24）A. UDP 报文　　B. TCP 报文　　C. SMTP 报文　　D. FTP 报文

试题（23）、（24）分析

本题考查 ASN.1、SNMP 方面的基本知识。

MIB 中的信息用 ASN.1 规定的格式表示，每个数据由标签（Tag）、长度（Length）和值（Value）三部分外加一个可选的结束标识部分构成，如下图所示，称为 TLV 表示法。每个字段都是一个或多个字节。



对二进制位串，其“值”部分的第一个字节表示最后一个字节中无效位的数量。

参考答案

（23）D　　（24）A

试题（25）、（26）

IntServ 是 Internet 实现 QoS 的一种方式，它主要依靠＿（25）＿，其实现资源预留的是＿（26）＿。

（25）A. SLA　　B. RSVP　　C. RTP　　D. MPLS

（26）A. 接纳控制器　　B. 调度器　　C. 分类器　　D. 路由选择协议

试题（25）、（26）分析

本题考查 QoS 及 IntServ 的基本知识。

IntServ 实现 QoS 的基本思想是，在通信开始之前利用资源预留方式为通信双方预留所需的资源，保证所需要的 QoS。

参考答案

（25）B　（26）A

试题（27）～（33）

某大学拟建设无线校园网，委托甲公司承建。甲公司的张工程师带队去进行需求调研，获得的主要信息有：

校园面积约 4km^2，室外绝大部分区域、主要建筑物内实现覆盖，允许同时上网用户数量为 5000 以上，非本校师生不允许自由接入，主要业务类型为上网浏览、电子邮件、FTP、QQ 等，后端与现有校园网相连，网络建设周期为 6 个月。

张工据此撰写了需求分析报告，其中最关键的部分应是＿（27）＿。为此，张工在需求报告中将会详细地给出＿（28）＿。

张工随后提交了逻辑网络设计方案，其核心内容包括：

① 网络拓扑设计

② 无线网络设计

③ 安全接入方案设计

④ 地址分配方案设计

⑤ 应用功能配置方案设计

针对无线网络的选型，最可能的方案是＿（29）＿。

针对室外供电问题，最可能的方案是＿（30）＿。

针对安全接入问题，最可能的方案是＿（31）＿。

张工在之前两份报告的基础上，完成了物理网络设计报告，其核心内容包括：

① 物理拓扑及线路设计

② 设备选型方案

在物理拓扑及线路设计部分，由于某些位置远离原校园网，张工最可能的建议是＿（32）＿。

在设备选型部分，针对学校的特点，张工最可能的建议是＿（33）＿。

（27）A. 高带宽以满足大量用户同时接入

B. 设备数量及优化布局以实现全覆盖

C. 安全隔离措施以阻止非法用户接入

D. 应用软件配置以满足应用需求

（28）A. 校园地图及无线网络覆盖区域示意图

B. 访问控制建议方案

C. 应购置或配置的应用软件清单

D. 对原校园网改造的建议方案

（29）A. 采用基于 WLAN 的技术建设无线校园网

B. 采用基于固定 WiMAX 的技术建设无线校园网

C. 直接利用电信运营商的 3G 系统
D. 暂缓执行，等待移动 WiMAX 成熟并商用
（30）A. 采用太阳能供电
B. 地下埋设专用供电电缆
C. 高空架设专用供电电缆
D. 以 PoE 方式供电
（31）A. 通过 MAC 地址认证
B. 通过 IP 地址认证
C. 在应用层通过用户名与密码认证
D. 通过用户的物理位置认证
（32）A. 采用单模光纤及对应光端设备连接无线接入设备
B. 采用多模光纤及对应光端设备连接无线接入设备
C. 修改无线接入设备的位置，以利用 UTP 连接无线接入设备
D. 将无线接入设备设置为 Mesh 和 Ad hoc 工作模式，实现中继接入
（33）A. 采用基于 802.11n 的高性价比胖 AP
B. 采用基于 802.11n 的高性价比瘦 AP
C. 采用基于 3G 的高性价比设备
D. 采用基于 LTE 的高性价比设备

试题（27）～（33）分析

本题考查逻辑网络需求设计、逻辑网络设计、物理网络设计的相关知识。

从用户的主要需求可以看出，该无线网络覆盖范围较大、用户数量多，其应用类型为普通应用。因此应重点关注设备数量及优化布局以实现全覆盖的问题，在需求报告中应给出校园地图及无线网络覆盖区域示意图。

综合现有技术成熟度及其普及程度、性能、成本等因素，WLAN 技术应是首选方案，其室外 AP 应首选 PoE 方式以减少供电线路。

因用户数量多且变化频繁、流动性强，采用应用层认证接入应是最佳的方案。

因 AP 较多且很多 AP 在室外，为方便管理，性能高的瘦 AP 应是首选方案。

参考答案

（27）B　（28）A　（29）A　（30）D　（31）C　（32）A　（33）B

试题（34）～（36）

工程师利用测试设备对某信息点已经连接好的网线进行测试时，发现有 4 根线不通，但计算机仍然能利用该网线连接上网。则不通的 4 根线可能是__（34）__。某些交换机级联时，需要交换 UTP 一端的线序，其规则是__（35）__，对变更了线序的 UTP，最直接的测试方式是__（36）__。

（34）A. 1-2-3-4　B. 5-6-7-8　C. 1-2-3-6　D. 4-5-7-8

（35）A. 1⟷2，3⟷4　　B. 1⟷2，3⟷6
C. 1⟷3，2⟷6　　D. 5⟷6，7⟷8

（36）A. 采用同样的测试设备测试　　B. 利用万用电表测试
C. 一端连接计算机测试　　D. 串联成一根线测试

试题（34）～（36）分析

本题考查网络布线与测试方面的基本知识。

根据相关标准，10Mbps 以太网只使用 4 根线，UTP 电缆中的 1-2-3-6 这 4 根线是必须的，分别配对成发送和接收信道。具体规定为：1、2 线用于发送，3、6 线用于接收。但百兆以太网、千兆以太网需要使用全部 8 根线。

当需要交换线序时，将线的其中一端的 1⟷3，2⟷6 分别对调。

对变更了线序的 UTP 进行测试时，最简单的方法是利用万用表测试。

参考答案

（34）D　（35）C　（36）B

试题（37）

某楼层的无线路由器通过 UTP 连接至网络中心，并被配置了固定的合法地址，该楼层的计算机借助该无线路由器以无线方式访问 Internet。该楼层的计算机不定期地出现不能连接到 Internet 的情况，此时，在网络中心测试该无线路由器，显示一切正常。更换同型号的无线路由器后，仍然出现上述现象。每次只要重启无线路由器，则一切恢复正常。导致这一现象的最可能原因是__（37）__。

（37）A. 设备故障　　B. 设置不当
C. 无线信号干扰　　D. 网络攻击

试题（37）分析

本题考查网络故障分析与处理方面的基本知识。

针对本题的现象，说明有线线路、所有网络设备、用户计算机等都应该没有问题。最可能的原因应是针对 AP 的攻击导致的。

参考答案

（37）D

试题（38）、（39）

评估网络的核心路由器性能时，通常最关心的指标是__（38）__，与该参数密切相关的参数或项目是__（39）__。

（38）A. Mpps 值　　B. Mbps 值
C. 可管理 MAC 地址数　　D. 允许的 VLAN 数

（39）A. 传输介质及数据率　　B. 协议种类
C. 背板交换速度　　D. 内存容量及 CPU 主频

试题（38）、（39）分析

本题考查网络性能评估方面的基本知识。

对路由器，最重要的性能指标之一是单位时间内能转发的分组数，即 Mpps 值（每秒百万分组数），其保证条件之一是背板交换速度。

参考答案

（38）A　（39）C

试题（40）～（45）

张工应邀为一炼钢厂的中心机房设计设备方案。其现状是：机房处于车间附近，车间具有很高的温度，所用设备具有很强的交流电流；控制系统基于计算机网络实现数据传输、存储；约有 2000 个监测点（通过多台 PLC 设备实现），每个监测点每 2ms 取样一次 4 字节的监测数据，通过网络发送到网络中心，并以文件形式被保存到文件服务器上，所有监测数据需在服务器上保存半年以上；对各种设备的控制信号通过同一网络传输到各监控点上；各种监测数据可在异地通过公用网络同步查看并进行实时分析。张工的方案中，将设备分为三类：一是服务器类，设计了文件服务器、数据库服务器、控制服务器、监控服务器等 4 个主要服务器；二是网络设备类，设计了一个路由器、5 台千兆交换机等主要设备；三是辅助类，包括 UPS、机房监控系统、空调等主要设备，另外计划配置有关软件系统。

文件服务器采用 RAID5 冗余模式、容量为 1TB 的硬盘构建，则应配置的硬盘数至少为 （40） ，优先采用的结构是 （41） 。

监控服务器负责接收、处理监测数据，其恰当的机型是 （42） 。

所配置的监测数据分析软件应具备的最基本功能是 （43） 。

交换机最必要的配置是 （44） 。

根据上述需求，至少应增加的一台设备是 （45） 。

（40）A. 65　　B. 78　　C. 86　　D. 96

（41）A. IPSAN　　B. FCSAN　　C. NAS　　D. DAS

（42）A. 大规模 Cluster　　B. 小规模 Cluster　　C. 大规模 SMP　　D. 小规模 SMP

（43）A. FFT 变换　　B. 趋势图显示　　C. 带通滤波　　D. 3D 图形

（44）A. 双电源　　B. 光纤模块　　C. VLAN 功能　　D. ACL 功能

（45）A. 防火墙　　B. IPS　　C.Web 服务器　　D. FTP 服务器

试题（40）～（45）分析

本题考查重要的网络资源设备及机房设计的有关知识。

文件服务器的硬盘容量的最低需求为能存储半年的数据：183（天）×86400（秒/天）×500（次采样/秒）×4（B/次采样）×2000≈63TB。应该将磁盘作为文件服务器的附属存储设备，因此首选 NAS 结构。

监控服务器负责接收、处理监测数据，选用小规模 SMP 就能满足要求。

对实时数据监测的最重要功能之一是监测其变化趋势，因此趋势图分析是必不可少的。

因数据的实时性要求很高，且工作环境电磁干扰严重，因此应首选光纤作为信号传输介质。

由于允许其他用户通过 Internet 访问监测数据，因此必须提供最基本的安全保证，而防火墙可限制非法用户访问。

参考答案

（40）D　（41）C　（42）D　（43）B　（44）B　（45）A

试题（46）

主动防御是新型的杀病毒技术，其原理是<u>（46）</u>。

（46）A. 根据特定的指令串识别病毒程序并阻止其运行

B. 根据特定的标志识别病毒程序并阻止其运行

C. 根据特定的行为识别病毒程序并阻止其运行

D. 根据特定的程序结构识别病毒程序并阻止其运行

试题（46）分析

本题考查病毒与木马的基本概念。

主动防御技术是根据特定行为判断程序是否为病毒。

参考答案

（46）C

试题（47）

一些病毒程序如 CIH 声称能破坏计算机的硬件，使得计算机彻底瘫痪。其原理是<u>（47）</u>。

（47）A. 生成高电压烧坏器件　B. 生成大电流烧坏器件

C. 毁坏 ROMBIOS 程序　D. 毁坏 CMOS 中的内容

试题（47）分析

本题考查病毒的基本概念。

通常，病毒程序并不能毁坏硬件本身，只是破坏硬件中的软件。

参考答案

（47）D

试题（48）、（49）

IDS 是一类重要的安全技术，其实现安全的基本思想是<u>（48）</u>，与其他网络安全技术相比，IDS 的最大特点是<u>（49）</u>。

（48）A. 过滤特定来源的数据包　B. 过滤发往特定对象的数据包

C. 利用网闸等隔离措施　D. 通过网络行为判断是否安全

（49）A. 准确度高　B. 防木马效果最好

C. 能发现内部误操作　　D. 能实现访问控制

试题（48）、（49）分析

本题考查 IDS 的基本知识。

IDS 的基本原理是通过分析网络行为（访问方式、访问量、与历史访问规律的差异等）判断网络是否被攻击及何种攻击。但这种分析并不能知道用户的各种突发性和变化的需求，因此很容易出现误判，并且对网络内部的误操作不能准确判断。

参考答案

（48）D　（49）C

试题（50）

很多系统在登录时都要求用户输入以图片形式显示的一个字符串，其作用是__（50）__。

（50）A. 阻止没有键盘的用户登录　　B. 欺骗非法用户

C. 防止用户利用程序自动登录　　D. 限制登录次数

试题（50）分析

本题考查加密与认证的基本方法。

很多系统在登录时都要求用户输入以图片形式显示的一个字符串，可防止非法用户利用程序自动生成密码登录，即用暴力方式破解密码。

参考答案

（50）C

试题（51）～（53）

椭圆曲线密码 ECC 是一种公开密钥加密算法体制，其密码由六元组 T=<p,a,b,G,n,h> 表示。用户的私钥 d 的取值为__（51）__，公钥 Q 的取值为__（52）__。

利用 ECC 实现数字签名与利用 RSA 实现数字签名的主要区别是__（53）__。

（51）A. 0～n–1 间的随机数　　B. 0～n–1 间的一个素数

C. 0～p–1 间的随机数　　D. 0～p–1 间的一个素数

（52）A. Q=dG　　B. Q=ph

C. $Q=a^b G$　　D. $Q=h^n G$

（53）A. ECC 签名后的内容中没有原文，而 RSA 签名后的内容中包含原文

B. ECC 签名后的内容中包含原文，而 RSA 签名后的内容中没有原文

C. ECC 签名需要使用自己的公钥，而 RSA 签名需要使用对方的公钥

D. ECC 验证签名需要使用自己的私钥，而 RSA 验证签名需要使用对方的公钥

试题（51）～（53）分析

本题考查椭圆曲线密码 ECC 的基本知识。

ECC 规定用户的私钥 d 为一个随机数，取值范围为 0～n–1。公钥 Q 通过 dG 进行计算（通过 Q 反算 d 是不可行的）。

RSA 实现签名的原理是分别利用自己的私钥和对方的公钥加密，签名后的内容是加

密后的密文。而 ECC 的签名原理是利用密钥生成两个数附加在原始明文后一同发送。

参考答案

（51）A　（52）A　（53）B

试题（54）、（55）

用于保护通信过程的初级密钥在分配和传输过程中通常的形式是__（54）__，利用其加密或解密时，应实施的操作是__（55）__。

（54）A. 一次一密的明文　　B. 一次一密的密文
C. 可多次使用的密文　　D. 不限次数的密文

（55）A. 利用二级密钥解密出原始密钥
B. 利用主密钥解密出原始密钥
C. 利用二级密钥和主密钥解密出原始密钥
D. 利用自身私钥解密出原始密钥

试题（54）、（55）分析

本题考查密钥管理的基本知识。

初级密钥是最低级的密钥，为提高其安全性，通常采用一次一密的传送方式，即一个密钥只能使用一次，且需高一级密钥对其解密后才能用于解密。

参考答案

（54）A　（55）A

试题（56）、（57）

利用交换机的 ACL 功能可增强网络的安全性和功能，其中不能实现的功能是__（56）__，交换机上的 RADIUS 不能实现的功能是__（57）__。

（56）A. 限制每个端口的数据率
B. 限制每个端口的流量
C. 限制每个端口可接入的 IP 地址
D. 限制每个端口可接入的 MAC 地址

（57）A. 用户名认证
B. 用户密码认证
C. 用户接入权限认证
D. 流量控制

试题（56）、（57）分析

本题考查访问控制的基本知识。

ACL 是新型交换机具有的、实现访问控制的功能，具有限制每个端口的数据率、限制每个端口可接入的 IP 地址、限制每个端口可接入的 MAC 地址等很多功能，但一般都不能限制每个端口的流量。

交换机的 RADIUS 可实现安全访问控制，不对流量进行控制。

参考答案

（56）B　（57）D

试题（58）～（60）

种植、自启动、隐藏是木马程序的三大关键技术。由于杀病毒软件的存在，隐秘种植木马并不容易，其中一种较好的方法是__（58）__。在 Windows 系统中，为实现木马的自动启动，通常的方法是将其放于__（59）__中。为避免用户发现木马的存在，较好的隐藏方法__（60）__。

（58）A. 当用户不在现场时派人安装
B. 当用户下载合法软件时顺便下载并安装
C. 当用户在线观看电影时下载并安装
D. 当用户打开邮件附件时安装

（59）A. autoexec.bat 文件　B. boot.ini 文件　C. config.sys 文件　D. 注册表

（60）A. 不显示自己的名称等信息
B. 把自己更名成操作系统中一个合法程序的名字
C. 伪装成一个系统服务
D. 需要运行时启动，运行完后退出

试题（58）～（60）分析

本题考查有关木马的基本知识。

参考答案

（58）B　（59）D　（60）D

试题（61）、（62）

为防止服务器遭攻击，通常设置一个 DMZ。有关外网、DMZ、内网三者之间的关系，应满足__（61）__。如果在 DMZ 中没有__（62）__，则访问规则可更简单。

（61）A. 外网可访问 DMZ，不能访问内网，DMZ 可访问内网和外网，内网可访问外网和 DMZ
B. 外网可访问 DMZ，可有条件访问内网，DMZ 可访问内网，不能访问外网，内网可访问 DMZ，不能访问外网
C. 外网可访问 DMZ，不能访问内网，DMZ 可访问外网，不能访问内网，内网可访问 DMZ 和外网
D. 外网可访问 DMZ，不能访问内网，DMZ 不能访问内网和外网，内网可有条件地访问 DMZ 和外网

（62）A. 邮件服务器　B. Web 服务器　C. DNS 服务器　D. 数据库服务器

试题（61）、（62）分析

本题考查网络隔离与 DMZ 方面的基本知识。

DMZ 通常是内网服务器的一个代理，用于替代内网服务器供外网用户访问，使得

内网服务器不暴露给外网用户。一旦 DMZ 中的服务器被攻击导致失效，可利用内网服务器快速恢复。

邮件服务器是内外网用户都要访问的服务器，当 DMZ 中没有邮件服务器时，可以完全限制 DMZ 与内网之间的联系，只允许内网到 DMZ 的单向访问，内网安全性进一步提高。

参考答案

（61）C　（62）A

试题（63）、（64）

高速、移动是未来计算机网络的重要特征，可作为未来无线广域网络技术的是__（63）__，其下行、上行的数据率将分别达到__（64）__。

（63）A. 3G　B. WiMAX　C. LTE　D. UWB

（64）A. 14.4Mbps、7.2Mbps　B. 52Mbps、26Mbps
C. 100Mbps、100Mbps　D. 326Mbps、86Mbps

试题（63）、（64）分析

本题考查广域网的基本知识。

LTE 即长期演进计划，是 3G 之后的下一代高速无线广域网技术，按现有技术规范，其上行、下行的数据率将分别达到 86 Mbps 和 326Mbps。随着技术的进步，该数据率一定会被突破。

参考答案

（63）C　（64）D

试题（65）

在项目施工前，首先要做一个进度计划，其中进度计划最常见的表示形式是__（65）__。

（65）A. 甘特图　B. Excel 表　C. 日历表　D. 柱状图

试题（65）分析

本题考查项目管理中的进度控制的基本知识。

甘特图是进行进度管理的最常用的工具，其通常形式是纵向表示项目，横向表示所需的时间。几乎所有的 IT 项目管理软件都具有甘特图功能。

参考答案

（65）A

试题（66）

网络工程项目质量管理的重要标准是__（66）__。

（66）A. CMM　B. GB 8567　C. ISO 9001　D. ISO 14000

试题（66）分析

本题考查质量管理标准方面的基本知识。

ISO 9001 是重要的质量管理标准。ISO 9001 对设计开发到生产、安装及服务等全过

程提出了要求。

CMM（软件成熟度模型）是关于软件开发管理的一个模型，GB 8567 是中国关于软件开发过程的一个国家标准，主要是文档制作规范，ISO 14000 是环境管理系列标准。

参考答案

（66）C

试题（67）、（68）

乙公司中标承接了甲机构的网络工程集成项目，在合同中约定了因不可抗力因素导致工期延误而免责的条款，其中不被甲机构认可的一种因素是__（67）__。合同约定，甲乙双方一旦出现分歧，在协商不成时，可提交到相关机构裁定，一般优先选择的裁定机构是__（68）__。

（67）A. 施工现场遭遇长时间雷雨天气　　B. 物流公司车辆遭遇车祸
　　C. 乙方施工队领导遭遇意外情况　　D. 甲机构相关负责人变更

（68）A. 甲机构所在地的仲裁委员会　　B. 乙公司所在地的仲裁委员会
　　C. 甲机构所在地的人民法院　　D. 乙公司所在地的人民法院

试题（67）、（68）分析

本题考查项目管理中合同制定与管理方面的基本知识。

不可抗力因素通常是指自然、环境或不可控制的第三方因素，乙方自身的因素应是可控因素，一般都不会被认同为不可抗力因素。

当发生分歧且协商不成时，一般情况下都是优先选择仲裁机构裁决，这样便于双方进一步协商且有利于控制矛盾升级。

在市场经济条件下，因甲方通常具有主动权，所以一般选择甲方所在地的仲裁委员会或法院。

参考答案

（67）C　　（68）A

试题（69）

甲公司委托销售部的客户经理张经理代表公司参加一个网络工程项目的投标，张经理在规定时间内提交了投标文件。招标单位在详细审查了投标文件后向张经理提出了一个简单的问题：你是甲公司的代表吗？张经理于是赶紧找到招标单位的王科长作证，以证明他是甲公司的。对甲公司的此次投标，最可能的结果是__（69）__。

（69）A. 因在招标单位有重要的熟人而顺利入围进入下一轮
　　B. 因张经理没有书面授权而无法通过资格审查被淘汰
　　C. 因通过补交证明材料顺利进入下一轮
　　D. 因甲公司法人代表随后赶到参与答辩而顺利进入下一轮

试题（69）分析

本题考查项目管理中招投标方面的基本知识。

按招标文件要求提交具有授权、公司盖章的各种书面材料是投标的唯一合法材料，依靠熟人作证不能作为有法律效力的证明材料。

参考答案

（69）B

试题（70）

M/M/1 排队论模型是分析网络性能的重要工具，假定通信量强度为 ρ（信道的平均繁忙程度），则节点中的等待输出的平均分组数为__（70）__。

（70）A. 1/（1−ρ）　B. ρ/（1−ρ）　C.（1−ρ）/ρ　D. ρ

试题（70）分析

本题考查排队论的应用。

排队论是分析网络性能最重要的工具之一。

参考答案

（70）B

试题（71）～（75）

A Bluetooth device can be either a master or a slave and any of the devices within a __（71）__ can be the master. There is only one master and there can be up to __（72）__ active slave devices at a time within a single network. In addition, a device may be a standby slave or a parked slave. There can be up to __（73）__ parked slaves. If there are already maximum number of active slaves, then a parked slave must wait until one of the active slaves switches to __（74）__ mode before it can become active. Within a network, all __（75）__ communications are prohibited.

（71）A. Wireless LAN　B. Wireless MAN
　　C. Cellular radio network　D. Piconet

（72）A. 7　B. 15　C. 63　D. 255

（73）A. 127　B. 255　C. 511　D. 1023

（74）A. master　B. standby slave　C. parked slave　D. active slave

（75）A. master-to-master　B. master-to-slave
　　C. slave-to-slave　D. slave-to-master

参考译文

蓝牙设备可以是一个主设备，也可以是一个从设备，位于__（71）__中的任一设备都可以成为主设备。在一个网络中只有一个主设备，最多有__（72）__个激活的从设备。另外，一个设备可以是活跃的从设备或是休眠的从设备，最多有__（73）__个休眠的从设备。如果已有最大数量的活跃从设备，那么，一个休眠的从设备就必须等到某活跃从设备切换到__（74）__模式后才能被激活。在一个网络内，所有的__（75）__通信都是被禁止的。

参考答案

（71）D　（72）A　（73）B　（74）C　（75）C

第 8 章　2010 下半年网络规划设计师下午试卷 I 试题分析与解答

试题一（共 25 分）

阅读以下关于某省电子政务网络平台的叙述，回答问题 1、问题 2 和问题 3。

某省准备建立电子政务网络平台，实现全省上下各级部门之间的信息交换和资源共享。遵照《国家信息化领导小组关于推进国家电子政务网络建设的意见》的要求，电子政务网络分为电子政务外网和电子政务内网，该省即将建设的网络平台被定性为“非涉密”的电子政务外网。在第一期工程中，主要建设覆盖省直部门和各地市州的电子政务外网省级部分。电子政务外网是办公自动化、会议通知、行政审批、电子监察等跨部门应用系统的运行网络，还是一个网络承载平台，可以承载各类 VPN。例如，在当前的省级外网平台建设中，外网平台就需要承载两个 VPN：（1）互连各个部门的国库支付 VPN；（2）互连各个部门的视频监控 VPN。

【问题 1】（6 分）

电子政务外网承载 VPN，可以采用 L2TP、IPSec 和 MPLS VPN 三类技术，请对三种技术建设 VPN 进行比较，比较内容如表 1-1 所示。

表 1-1　VPN 技术比较

比较项目	L2TP	MPLS VPN	IPSec	备注
隧道协议层次				对隧道的协议层次进行比较
是否支持数据加密				
设备的要求				比较网络核心、边缘设备的协议支持要求
是否支持移动 VPN 客户端				

【问题 2】（6 分）

各地市州、各省直部门在接入电子政务外网平台时，需要配置接入路由器、防火墙、前置服务器，请考虑如下连接要求，并添加相应的连接线路或设备，给出接入电子政务外网的设备连接图。

（1）部门网络与电子政务外网之间为逻辑隔离；

（2）部门应用系统主动把数据推送至前置服务器，数据中心在进行数据获取时，不允许进入部门网络；

（3）在调试防火墙的各类过滤规则时，不会对电子政务外网的路由造成影响；

（4）可根据用户负载的需要，随时添置前置服务器。

【问题 3】（13 分）

如图 1-1 所示，省级电子政务外网平台承载了两个 VPN，分别为国库支付 VPN 和

视频监控 VPN。请从以下方面描述电子政务外网 PE 路由器上的 MPLS VPN 配置内容：

- VPN 接口配置
- PE-CE 配置
- OSPF 配置
- MPLS 配置

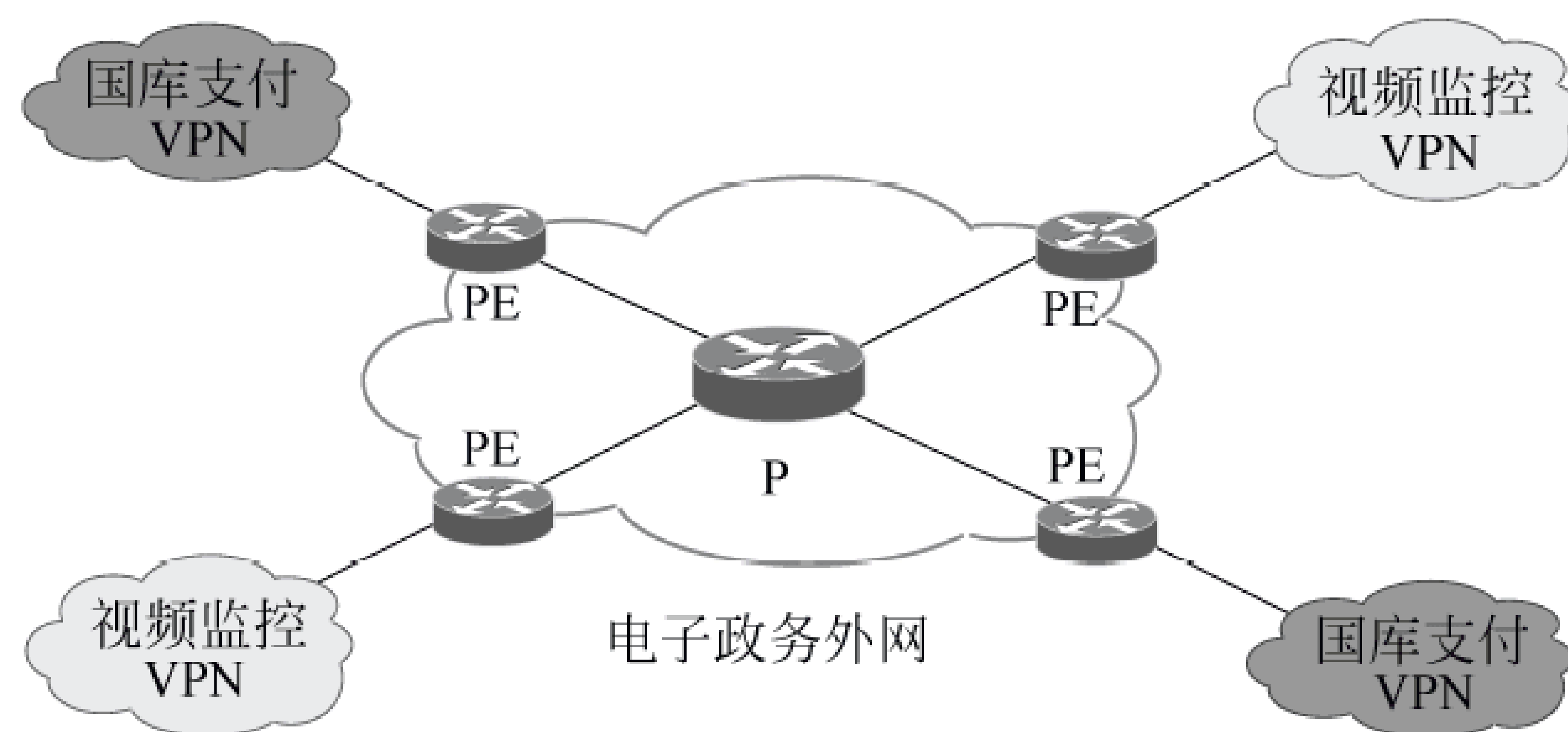


图 1-1　电子政务外网承载 VPN 示意图

试题一分析

本题涉及 MPLS 技术、MPLS VPN 等领域的内容。

【问题 1】

VPN（Virtual Private Network，虚拟专用网）就是利用 Internet 或其他公共互联网络的基础设施建立专用数据传输通道，将远程的分支机构、移动办公人员等连接起来，实现不同网络的组件和资源之间的相互连接，是通过隧道技术在公共数据网络上虚拟出一条点到点的专线技术。

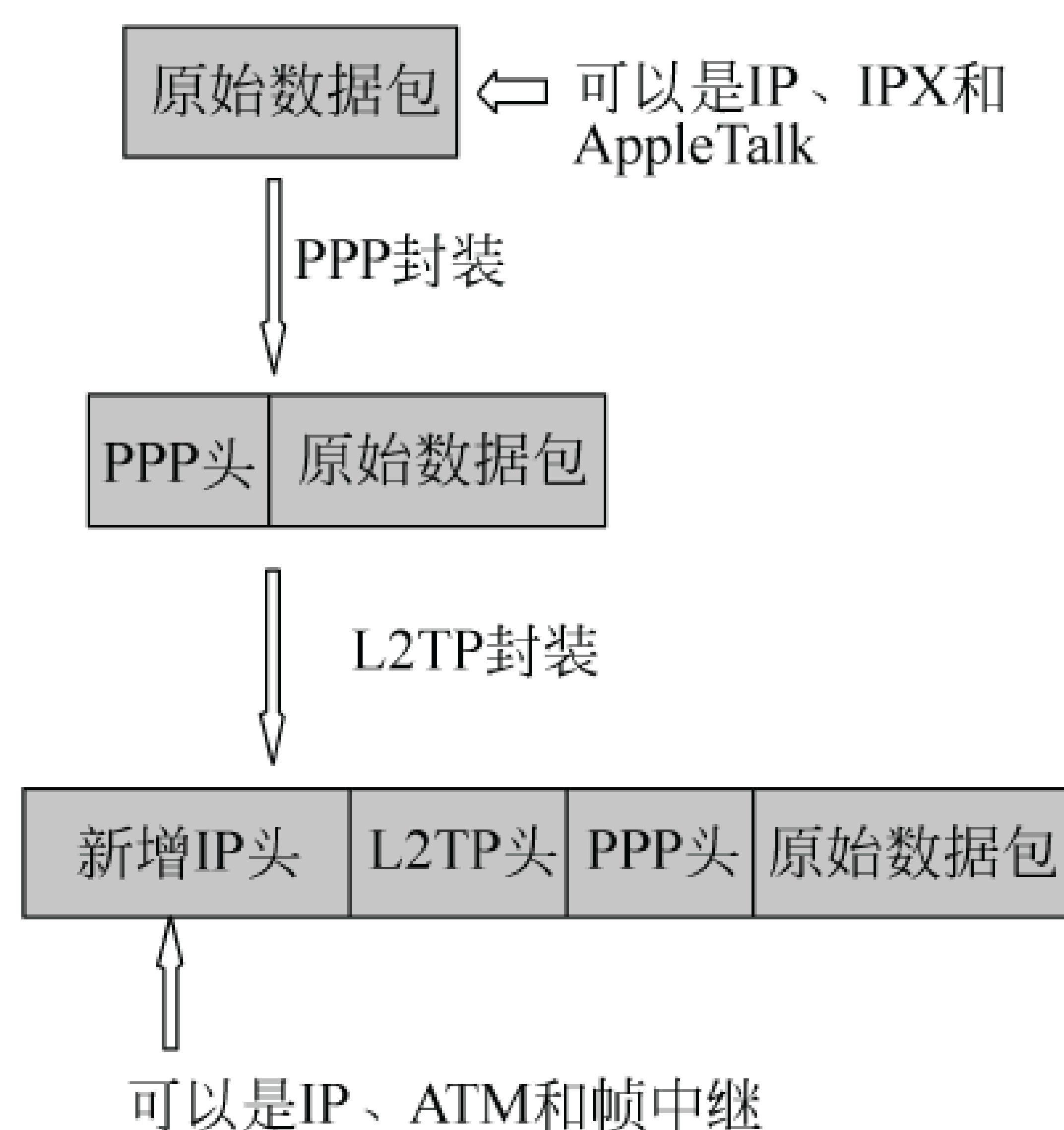
在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。

VPN 主要采用 4 项技术来保证安全，这 4 项技术分别为隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）、认证技术（Authentication）。

隧道技术就是利用隧道协议对隧道两端的数据进行封装的技术。利用一种协议来传输另外一种协议的技术，共涉及三种协议，包括乘客协议、隧道协议和承载协议，隧道协议可以分别是第二层或第三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中；这种双层封装方法形成的数据包靠第二层协议进行传输；第二层隧道协议有 L2F、PPTP、L2TP 等。第三层隧道协议则借助于网络层协议来进行封装，典型代表是 IPSec；IPSec 本身不是隧道协议，但由于其提供的认证、加密功能适用于建立 VPN 环境，它既能提供 LAN 间 VPN，也能提供远程访问型 VPN。而 MPLS VPN 则是一种借助于标签交换技术、利用公用 MPLS 基础设施实现多个用户网络承载，是一种介于第二层和第三层之间的技术。

L2TP 协议：

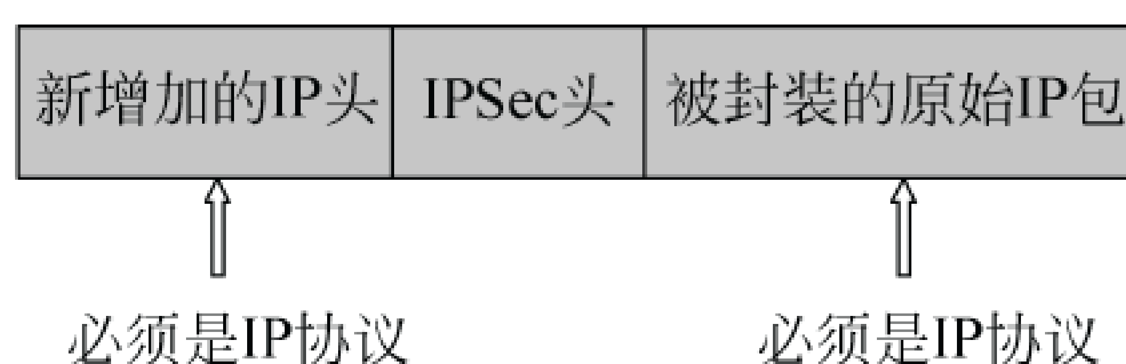
L2TP 封装的乘客协议是位于第二层的 PPP 协议，如下图所示。



L2TP 在数据传输过程中并没有对数据进行加密。

IPSec 协议：

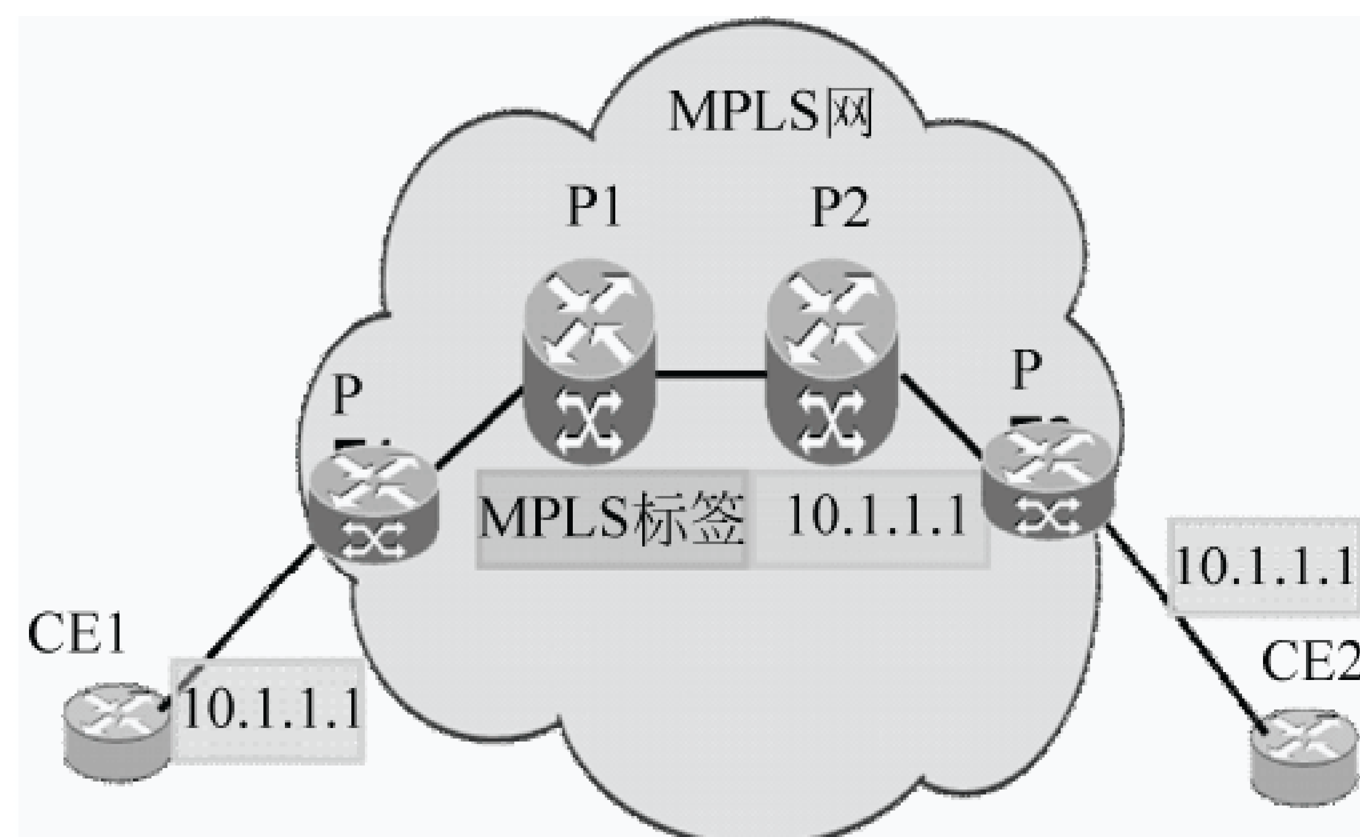
IPSec 只能工作在 IP 层，要求乘客协议和承载协议都是 IP 协议，如下图所示。



IPSec 在传输数据过程中，可以对被封装的数据包进行加密和摘要等，以进一步提高数据传输的安全性。

MPLS VPN：

MPLS VPN 技术借助于一个公用的 MPLS 域，在入口边缘路由器为每个包加上 MPLS 标签，核心路由器根据标签值进行转发，出口边缘路由器再去掉标签，恢复原来的 IP 包，如下图所示。



MPLS 标签位于二层和三层之间，其协议封装如下图所示。

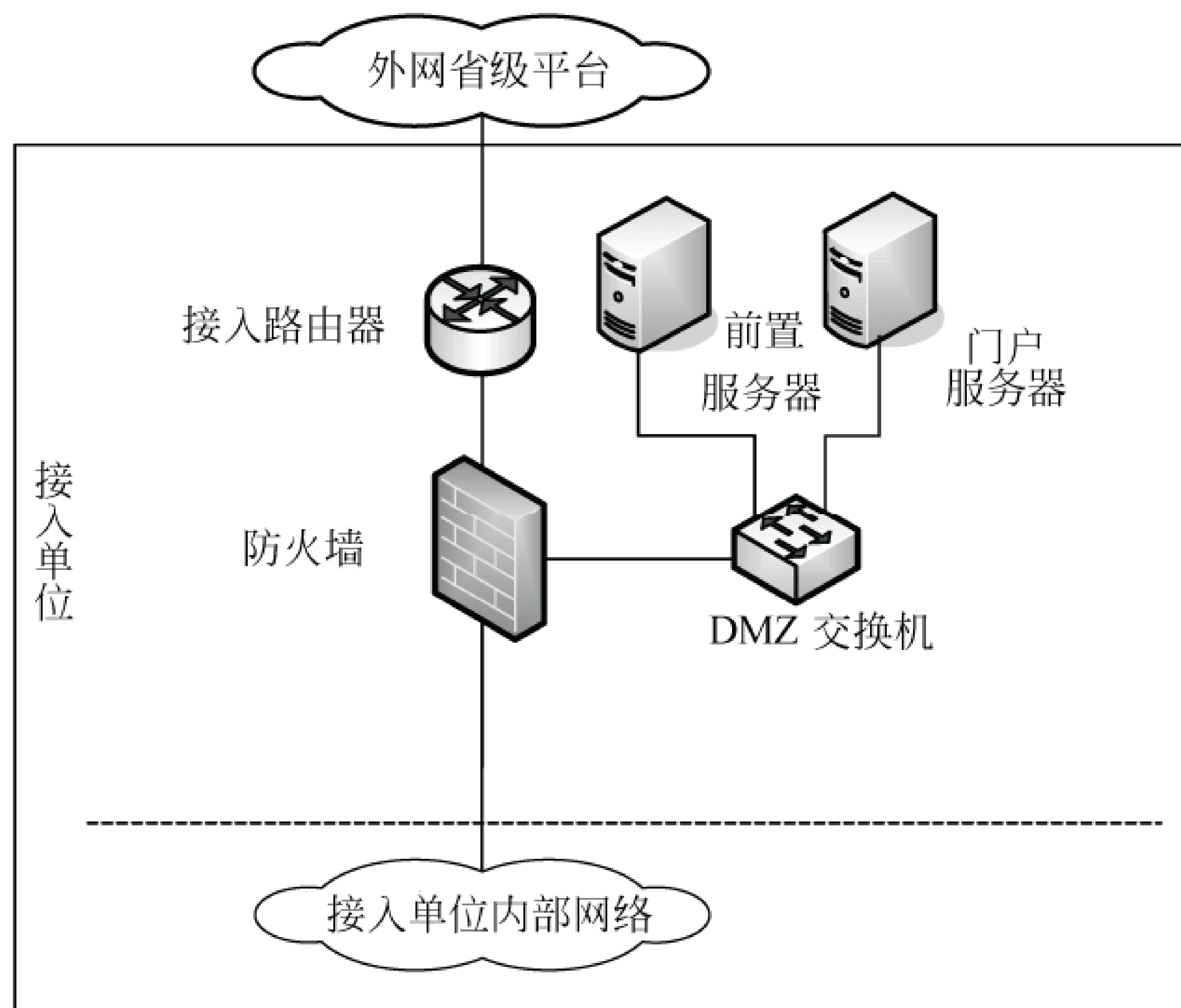


【问题 2】

电子政务网络一般分为电子政务内网和电子政务外网。其中电子政务外网是一个非涉密性质的网络，可以借助于特定的安全手段，实现普通信息和敏感信息的传递。电子政务外网在实现部门和下级单位接入时，主要采用逻辑隔离方式接入，即指两个网络之间存在着受控的网络协议传递，信息借助于防火墙或者具有过滤功能的路由器实现交换的方式。

逻辑隔离接入方式适用于大多数部门，其内部网络为实现对内部信息与资源实施保护，在受控的情况下与外网进行连接。由于电子政务网络建设主要为政务信息资源目录体系、政务信息资源交换体系、各类电子政务应用系统提供运行和承载环境；在实现部门网络接入的同时，需要为信息和数据的交换提供有效的技术支撑；因此，部门网络借助于防火墙或路由器完成与电子政务外网主干的连接，通过受控的网络协议实现信息交换。

传统意义上的部门逻辑接入方式如下图所示。



为完成各部门网络接入电子政务外网平台，必须配置特定的网络接入设备，这些设备主要包括接入路由器、防火墙、前置服务器、DMZ 交换机等。

- 接入路由器是实现单位接入的关键设备，通过运行路由算法，保持和外网平台的

连通性。

- 前置服务器是完成单位内部网络和外网平台数据交换的关键设备，通过前置数据库、交换中间件等实现数据的交换。
- 防火墙是完成逻辑隔离的关键设备，其强大的过滤机制、DMZ 区域设置等技术，保证了外网平台与单位网络之间的受控信息传递。
- DMZ 交换机用于扩展防火墙的 DMZ 区域，实现多台服务器在防火墙 DMZ 区域的接入。

【问题 3】

MPLS 最初是用来提高路由器的转发速度而提出的一个协议，MPLS 协议的关键是引入了标签（Label）交换概念；标签是一种短的、易于处理的、不包含拓扑信息、只具有局部意义的信息内容。

在 MPLS 网络中，IP 包在进入第一个 MPLS 设备时，MPLS 边缘路由器分析 IP 包的内容并且为这些 IP 包选择合适的标签；以后所有 MPLS 网络中的节点都是依据这个标签作为转发依据；当 IP 包最终离开 MPLS 网络时，标签被边缘路由器分离。

MPLS 在逻辑上可以分为 LER（Label Edge Router）和 LSR（Label Switching Router）。其中 LER 是 MPLS 网络同其他网络的边缘设备，它提供流量分类和标签映射、标签移除的功能；而 LSR 是 MPLS 网络的核心交换机，它提供标签交换、标签分发的功能。

作为一种高效的 IP 骨干网技术平台，MPLS 为实现 VPN 提供了一种灵活的、具有可扩展性的技术基础，并且具有网络配置简单、动态发现相邻节点、直接利用现有路由协议、具有良好的可扩展性等特点。

为支持基于 MPLS 的 VPN 特性，必须实现如下功能：

- LDP（Label Distribution Protocol）标签分布协议，是 MPLS 的信令协议，用以管理和分配标签；
- MPLS 转发模块，根据报文上的标签和本地映射表进行二、三层间交换；
- MBGP 和 BGP 扩展，用来传递 VPN 路由和承载 VPN 属性、QoS 信息、标签等内容；
- 路由管理的 VPN 扩展，建立多路由表，用以支持 VPN 路由。

在 MPLS VPN 的连接模型中，网络由运营商的骨干网与用户的各个 Site 组成，所谓 VPN 就是对 Site 集合的划分，一个 VPN 就对应一个由若干 Site 组成的集合。而 MPLS VPN 网络中的路由设备也相应分为三类：

- CE（Custom Edge）：用户 Site 中直接与服务提供商相连的边缘设备；
- PE（Provider Edge）：骨干网中的边缘设备，它直接与用户的 CE 相连；
- P 路由器（Provider Router）：骨干网中不与 CE 直接相连的设备。

MPLS VPN 的组成原理如下：

（1）MPLS VPN 的网络构造由服务提供商来完成。在这种网络构造中，由服务提供

商向用户提供 VPN 服务，用户感觉不到公共网络的存在，就好像拥有独立的网络资源一样。

（2）同样对于服务提供商骨干网络内部的 P 路由器，也就是不与 CE 直接相连的路由器而言，也不知道有 VPN 的存在，仅仅负责骨干网内部的数据传输。但其必须能够支持 MPLS 协议，并使能该协议。

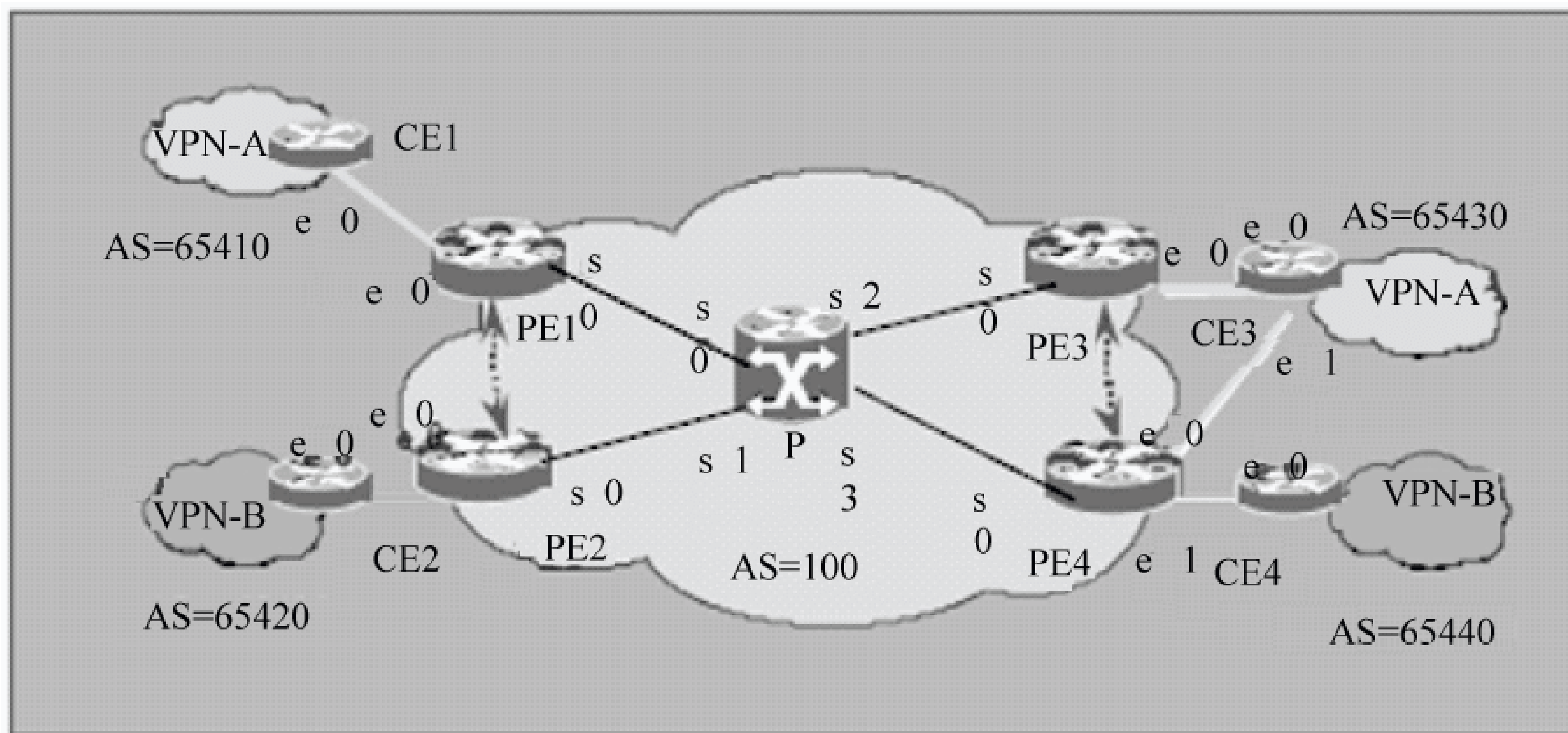
（3）所有的 VPN 的构建、连接和管理工作都是在 PE 上进行的。PE 位于服务提供商网络的边缘。从 PE 的角度来看，用户的一个连通的 IP 系统被视为一个 Site，每一个 Site 通过 CE 与 PE 相连，Site 是构成 VPN 的基本单元。

（4）一个 VPN 是由多个 Site 组成的，一个 Site 也可以同时属于不同的 VPN。属于同一个 VPN 的两个 Site 通过服务提供商的公共网络相连，VPN 数据在公共网络上传播，必须要保证数据传输的私有性和安全性。也就是说，从属于某个 VPN 的 Site 发送出来的报文只能转发到同样属于这个 VPN 的 Site 中去，而不能被转发到其他 Site 中去。

（5）同时，任何两个没有共同的 Site 的 VPN 都可以使用重叠的地址空间，即在用户的私有网络中使用自己独立的地址空间，而不用考虑是否与其他 VPN 或公网的地址空间冲突。所有这些就都需要依赖于 VRF（VPN Routing & Forwarding Instance）。

关于 VPN 路由转发实例（VPN Routing & Forwarding Instance）、路由标识（Route Distinguisher）、多协议 BGP（MultiProtocol BGP）、BGP 扩展团体属性（Extended Community）、BGP 路由刷新（Route Refresh）的详细技术内容，在本文中不做介绍，请参阅相关技术资料。

以下为问题 3 的 MPLS VPN 环境介绍及 MPLS VPN 的有关配置。



图中，s0 表示第 0 号串口，e0 表示第 0 号以太网口；P 路由器分别通过 s0、s1、s2、s3 与 PE1、PE2、PE3、PE4 相连；各用户网络的 AS 号码分别为 65410、65420、65430、65440，核心网络的 AS 号码为 100；VPN-A 为国库支付 VPN，VPN-B 为视频监控 VPN。

PE1 的配置：

```
# VRF 配置
Quidway#config terminal
#进入到配置模式
Quidway(config)#ip vrf vpna
#创建 VPN 实例 VPNA
Quidway(config-vrf)#rd 100:1
#配置 VPNA 的 rd 为：100:1
Quidway(config-vrf)#route-target both 100:1
#配置 rd 为 100:1 的站点可以双向接收此 VPN 路由
Quidway(config-vrf)#route-target import 100:2
#可以接收到 rd 为 100:2 站点发送过来的 VPN 路由
Quidway(config-vrf)#route-target export 100:3
#配置 rd 为 100:3 的站点可以接收此 VPN 路由
Quidway(config-vrf)#exit
#退出接口配置模式

# 接口配置
Quidway(config)#interface e 0
#进入到以态网 e0 口
Quidway(config-if-Ethernet0)#ip vrf forwarding vpna
#将接口添加到 VPNA 实例中
Quidway(config-if-Ethernet0)#ip address 168.1.1.2 255.255.0.0
#配置接口地址
Quidway(config-if-Ethernet0)#exit
#退出接口配置模式
Quidway(config)#interface s 0
#进入到串行接口 s0 口
Quidway(config-if-Serial0)#ip address 172.1.1.1 255.255.0.0
#配置接口地址
Quidway(config-if-Serial0)#exit
#退出接口配置模式

# PE-CE 配置
Quidway(config)#router bgp 100
#使能 BGP，自治系统号 100
Quidway(config-router-bgp)#address-family ipv4 vrf vpna
#在 BGP 的 IPv4 VRF VPNA 地址簇中引入路由信息
Quidway(config-router-af)#neighbor 168.1.1.1 remote-as 65410
#建立 IPv4 VRF VPNA 中的邻居，传递 VRF 路由
```

```
Quidway(config-router-af)#neighbor 168.1.1.1 activate
#建立 IPv4 VRF VPNA 中的邻居，并激活邻居
Quidway(config-router-af)#redistribute connected
#引入直连路由
Quidway(config-router-af)#exit-address-family
#退出当前配置模式
Quidway(config-router-bgp)#exit
#退出

# PE-PE 配置
Quidway(config)#router bgp 100
#使能 BGP，自治系统号 100
Quidway(config-router-bgp)#redistribute ospf metric 6
#引入 OSPF 路由并配置 metric 值为 6
Quidway(config-router-bgp)#address-family vpnv4
#配置 VPNV4 iBGP 路由，用以在 PE 之间传播 MBGP VPN 路由
Quidway(config-router-af)#neighbor 172.2.1.1 remote-as 100
#建立邻居
Quidway(config-router-af)#neighbor 172.2.1.1 activate
#激活邻居
Quidway(config-router-af)#neighbor 172.3.1.1 remote-as 100
Quidway(config-router-af)#neighbor 172.3.1.1 activate
Quidway(config-router-af)#neighbor 172.4.1.1 remote-as 100
Quidway(config-router-af)#neighbor 172.4.1.1 activate
Quidway(config-router-af)#exit-address
Quidway(config-router-bgp)#exit
# OSPF 配置
Quidway(config)#router ospf
#启用 OSPF 功能
Quidway(config-router-ospf)#network 172.1.1.0 0.0.255.255 area 0
#发布 OSPF 路由信息到区域 0
Quidway(config-router-ospf)#exit
# MPLS 配置
Quidway(config)#mpls lsr id 172.1.1.1
#配置 MPLS 的 lsr id 标识
Quidway(config)#mpls ldp
#启用 MPLS LDP 标签协议
Quidway(config-mpls-ldp)#exit
Quidway(config)#interface s 0
Quidway(config-if-Serial0)#mpls ldp enable
#在接口下启用 MPLS 标签功能
```

```
Quidway(config-if-Serial0)#exit
Quidway(config)#exit
Quidway#
```

CE1 的配置：

```
# 接口配置
Quidway#config terminal
Quidway(config)#interface e 0
Quidway(config-if-Ethernet0)#ip address 168.1.1.1 255.255.0.0
#配置以太口 IP 地址
Quidway(config-if-Ethernet0)#exit
# BGP 配置
Quidway(config)#router bgp 65410
Quidway(config-router-bgp)#neighbor 168.1.1.2 remote-as 100
#配置 BGP 邻居
Quidway(config-router-bgp)#exit
Quidway(config)#exit
Quidway#
```

P 路由器的配置：

```
# 接口配置
Quidway#config terminal
Quidway(config)#interface s 0
Quidway(config-if-Serial0)#ip address 172.1.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
Quidway(config)#interface s 1
Quidway(config-if-Serial0)#ip address 172.2.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
Quidway(config)#interface s 2
Quidway(config-if-Serial0)#ip address 172.3.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
Quidway(config)#interface s 3
Quidway(config-if-Serial0)#ip address 172.4.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
#配置各串口 IP 地址
# MPLS 配置
Quidway(config)#mpls lsr id 172.1.1.2
#配置 MPLS 的 lsr id 标识
Quidway(config)#mpls ldp
#启用 MPLS LDP 标签协议
```

```
Quidway(config-mpls-ldp)#exit
Quidway(config)#interface s 0
Quidway(config-if-Serial0)#mpls ldp enable
#在接口下启用 MPLS 标签功能
Quidway(config-if-Serial0)#exit
Quidway(config)#
Quidway(config)#interface s 1
Quidway(config-if-Serial0)#mpls ldp enable
Quidway(config-if-Serial0)#exit
Quidway(config)#
Quidway(config)#interface s 2
Quidway(config-if-Serial0)#mpls ldp enable
Quidway(config-if-Serial0)#exit
Quidway(config)#
Quidway(config)#interface s 3
Quidway(config-if-Serial0)#mpls ldp enable
Quidway(config-if-Serial0)#exit
Quidway(config)#
# OSPF 配置
Quidway(config)#router ospf
Quidway(config-router-ospf)#network 172.1.1.0 0.0.255.255 area 0
Quidway(config-router-ospf)#network 172.2.1.0 0.0.255.255 area 0
Quidway(config-router-ospf)#network 172.3.1.0 0.0.255.255 area 0
Quidway(config-router-ospf)#network 172.4.1.0 0.0.255.255 area 0
```

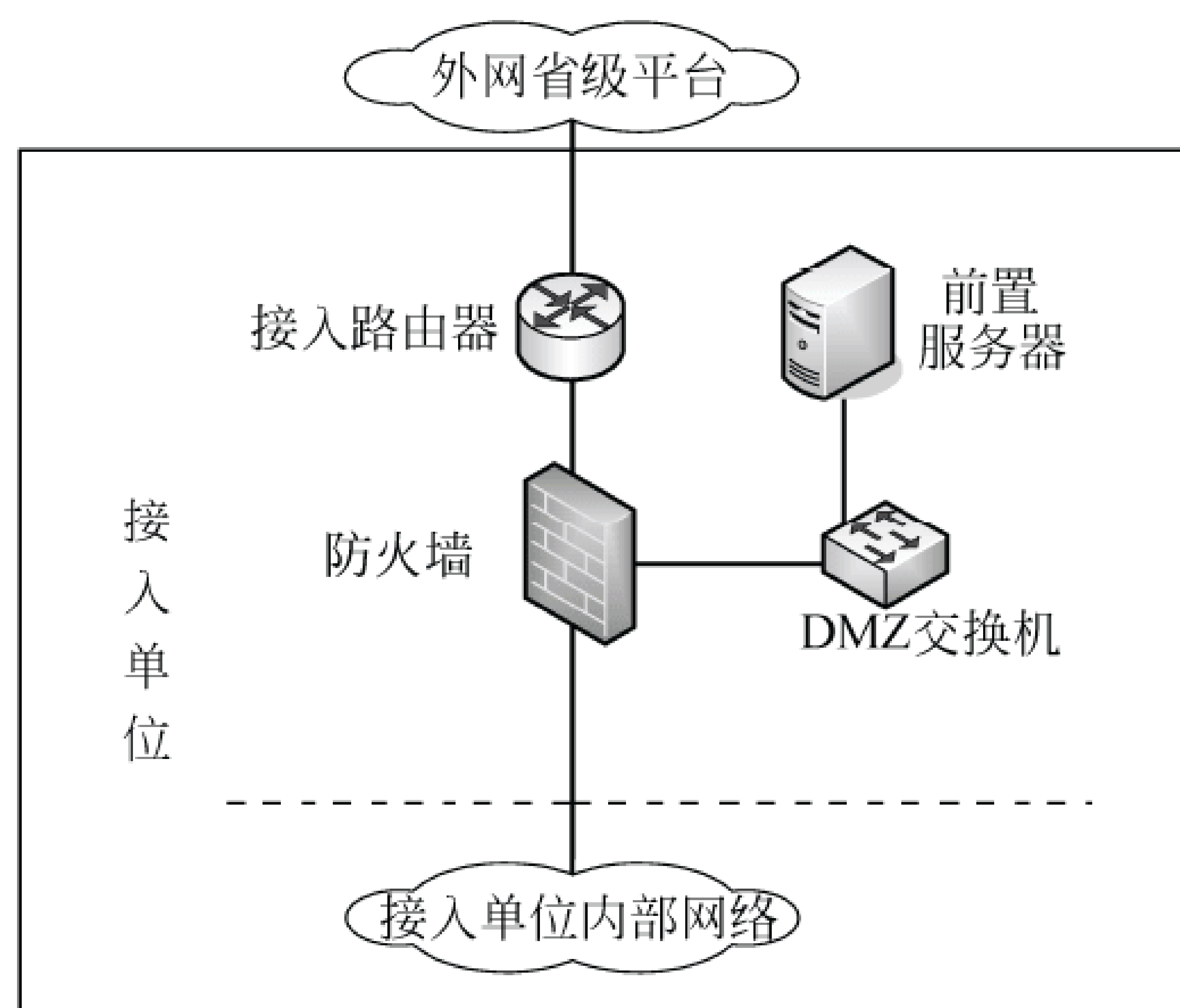
其他 PE 的配置与 PE1 相似，其他 CE 的配置与 CE1 相似，不重复列举。

参考答案

【问题 1】

比较项目	L2TP	MPLS VPN	IPSec	备　注
隧道协议层次	第二层	介于第二层和第三层之间（或两层半）	第三层	对隧道的协议层次进行比较
是否支持数据加密	不支持	不支持	支持	
设备的协议支持要求	只要求边缘设备支持 L2TP	要求边缘和核心设备都支持 MPLS	只要求边缘设备支持 IPSec	比较网络核心、边缘设备的协议支持要求
是否支持移动 VPN 客户端	支持	不支持	支持	

【问题 2】



画图要点：

接入路由器直接连接电子政务外网；

防火墙直接连接单位内部网络；

防火墙与接入路由器直接相连；

防火墙的 DMZ 口添置一台 DMZ 交换机；

前置服务器与 DMZ 交换机直接相连。

【问题 3】

（1）VPN 接口配置

将相应的接口加入 VPN 实例中；

进入接口配置模式，配置接口的 IP 地址。

（2）PE-CE 配置

启用路由协议 BGP，并设置自治区号；

在 BGP 的 IPv4 VRF 实例地址簇中引入路由信息；

建立 IPv4 VRF 实例的邻居关系，激活并传递 VRF 路由；

在 BGP 中引入直连路由。

（3）OSPF 配置

启用 OSPF 路由协议；

配置路由区域及网络地址信息。

（4）MPLS 配置

配置 MPLS 的 LSR ID 标识；

启用路由器的 MPLS LDP 标签协议；

在网络接口上启用 MPLS LDP 标签协议。

试题二（共 25 分）

阅读以下关于长江沿线某企业广域网络整合改造的需求，回答问题 1、问题 2 和问题 3。

长江沿线某物流企业 A 与 B 并购后组织机构合并，在此情况下，原有两个单位的信息网络的融合成为迫在眉睫的任务。在机构融合前，两个单位各自都有独立的广域网络：A 企业广域网覆盖重庆至上海，共 1 个核心节点（武汉长江南岸，100 个用户）、6 个二级节点（30 个用户）和 23 个三级节点（9 个用户）；B 企业广域网覆盖重庆至芜湖，共 1 个核心节点（武汉长江北岸，150 个用户）、11 个分支核心节点（11 个用户，包含 A 企业的二级节点）、200 多个扫描接入点（2 个终端）。两个广域网的主要传输通道都是通过 A 企业自建的 SDH 网络：A 企业广域网一二级节点间是 155MPOS 互联，二三级节点间采用 10M MSTP 或 2M 电路互联，少数链路为 40M MSTP；B 企业广域网核心和分支机构的互联采用 30～50M MSTP 互联，少数节点采用 4 个 2M 捆绑的电路连接。（注：所有 MSTP 电路使用仅用于实现二三级节点的点对点连接）

A 企业广域网承载着办公、视频监控、软交换、视频会议、广播控制系统等业务；B 企业广域网承载着办公、视频会议、数十个安全监管业务系统、CCTV、GPS 等物流监管系统等业务系统。

机构融合后，两个广域网再没有独立运行的必要了，因此要将两个广域网合并成一个网络，清理网络资产、简化网络结构（减少二级节点数量）、优化路由，使网络安全、高效、可靠、易维护、易管理。A 企业广域网结构如图 2-1 所示。

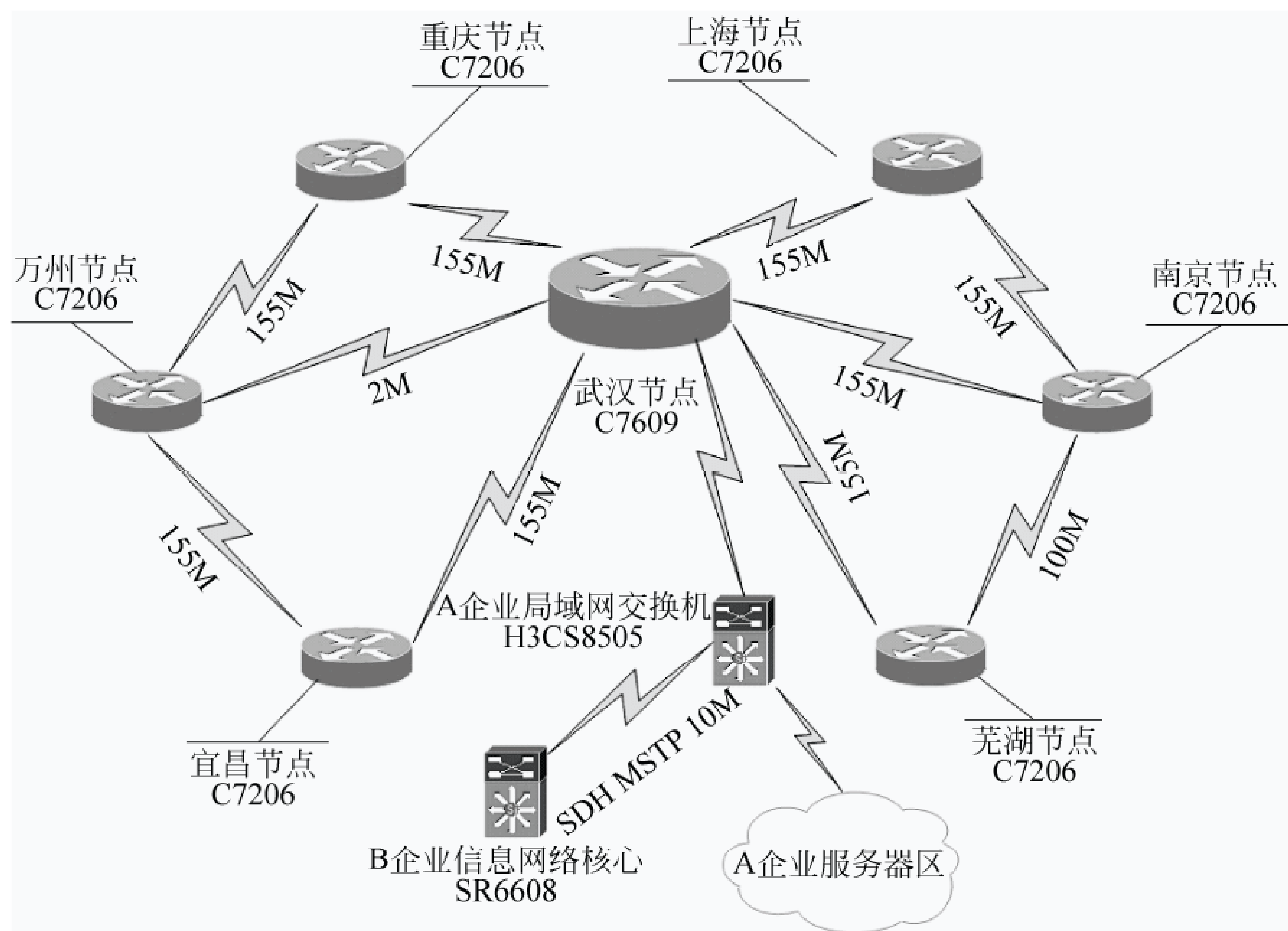


图 2-1　A 企业广域网结构

B 企业广域网结构如图 2-2 所示。

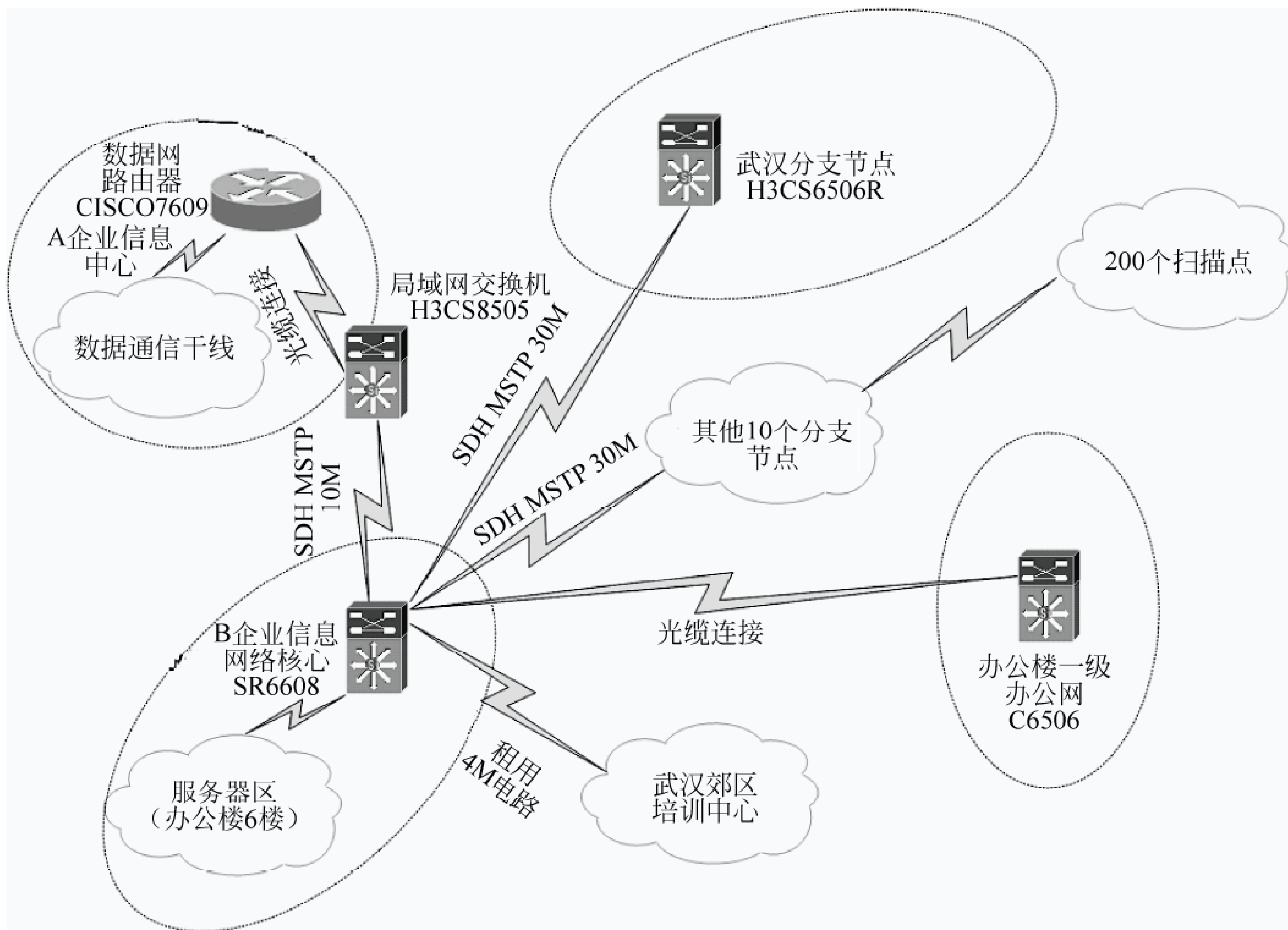


图 2-2　B 企业广域网结构

【问题 1】（10 分）

在不增加新设备、新链路的情况下，针对现有物理设备及线路给出整合解决方案的整体思路。要求：

（1）整合后的企业网络采用层次化设计、简化拓扑，实现核心节点、线路 N+1 冗余；

（2）整合后企业网络的二级节点包括重庆、万州、宜昌、芜湖、南京、上海以及位于武汉的“培训中心”和“武汉分支管理处”。

【问题 2】（8 分）

原 A 企业服务器地址采用 172.16.1.0/24 一个 C 类地址段，原 B 企业服务器地址采用 192.168.0.0/24、192.168.1.0/24 两个 C 类地址段。A、B 两企业用户地址和网络设备地址都采用 10.0.0.0/8 地址。要求在不影响业务的情况下采用层次化的地址分配方案合理规划地址（禁止使用 NAT 技术），并提供地址切换解决方案。

【问题 3】（7 分）

原 A 企业采用 OSPF 作为路由协议，协议进程规划为 1，二级节点作为 area0 边界

且往下分别归属于不同的 area。原 B 企业采用 OSPF 作为路由协议，协议进程规划为 10，分支节点作为 area0 边界且往下分别归属于不同的 area。合并前 A、B 两企业之间采用静态路由连接。要求提供两种基于 OSPF 协议的路由整合方案思路，并比较两种整合思路的优缺点。

试题二分析

本题涉及网络升级改造、性能优化等方面的内容。

【问题 1】

在进行企业网络整合改造之前，必须明确企业网络的现状，包括以下内容：

- 待整合网络的网络结构；
- 各网络节点的设备清单；
- 设备接口及连接情况；
- 待整合网络 IP 地址规划；
- 待整合网络路由规划。

在了解了网络现状之后，应制定网络整合的整体目标，本题中网络改造的整体目标是原有长江沿线的物流企业 A 和 B 的网络合并为一个网络，建设完成一地一中心、结构层次化网络，为物流企业日常办公及各应用系统提供快捷、可靠、稳定的统一的网络平台。

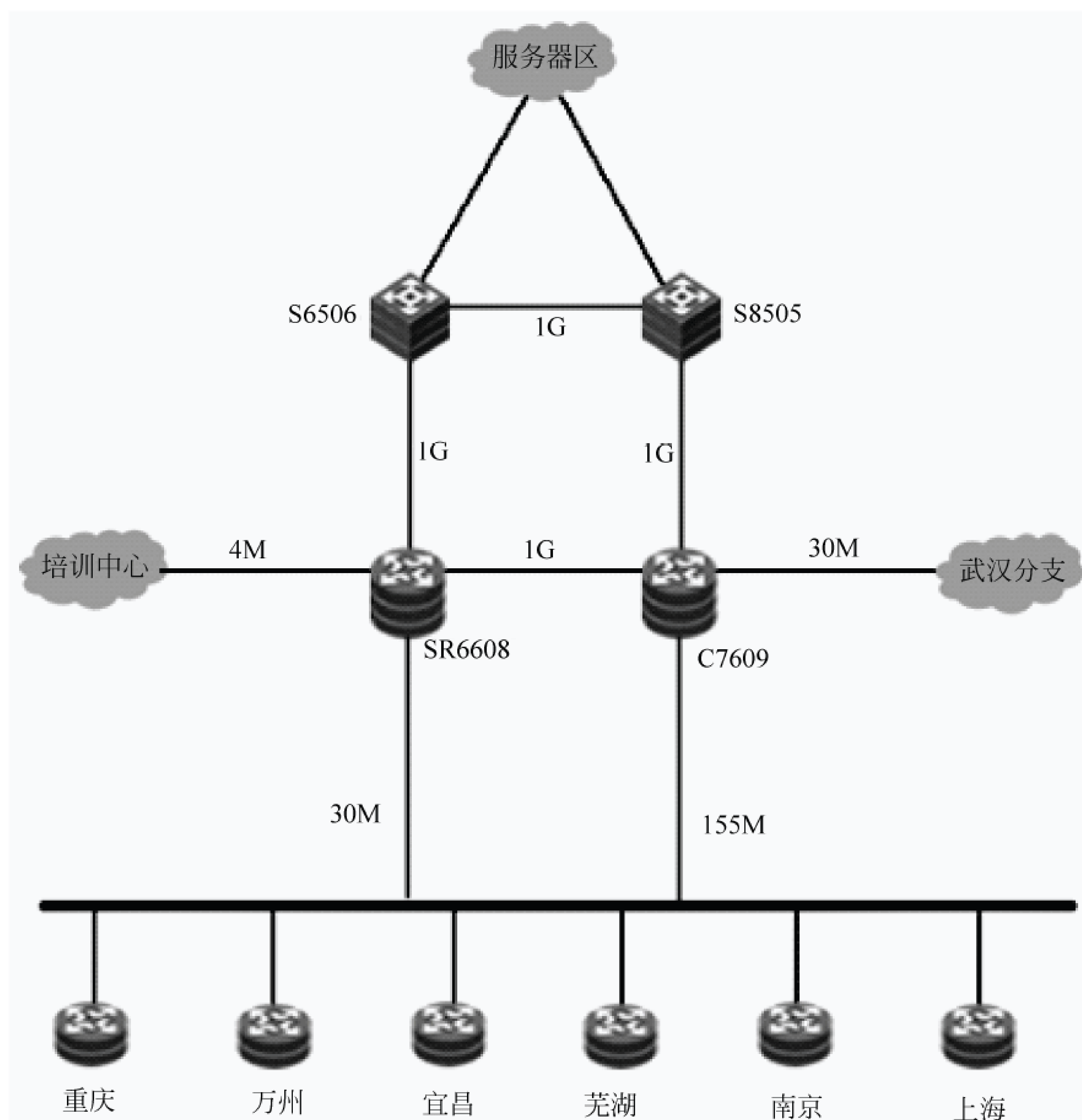
为实现网络整合的整体目标，还需要对网络平台的需求进行分析，需要包括以下内容：

- 业务需求分析，主要包括网络需要承载的业务系统；
- IT 资源利用分析，包括线路资源、网络设备资源、IP 地址资源；
- 整合后的网络结构分析；
- 整合后的网络路由规划分析；
- 改造的可行性分析，包括必要性、技术可行性、风险性等。

基于以上分析，形成整合改造方案。在本题中，可以采用如下的整体思路：

- 武汉的核心路由设备迁移到一个核心机房，并迁移原有与二级设备的链路；
- 所有服务器、核心交换机迁移到武汉的核心机房，并实现服务器区与两台核心交换机的默认网关冗余；
- 统一采用二级、三级节点方式，打乱原有连接方式；对 8 个二级节点以外的节点都降级为三级节点；对原 A 企业三级节点、B 企业扫描接入点采用就近接入原则或者就近线路迁移原则，形成三级网络结构；
- 原有 155M 线路作主用，30M 线路作备用。

最终可以形成新的网络结构，如下图所示。



【问题 2】

整合改造方案中，IP 地址规划是一个关键性问题，整合后的 IP 地址规划应依据科学性、系统性、完整性及可扩展性的代码分类原则，同时还应考虑如下思路：

- IP 地址资源以地域划分、行政隶属关系和业务种类为层次，分割为大小不同、用途各异的地址块单元；
- 实现地址的层次化划分，以利于路由信息的聚合，减少路由表长度；
- 充分利用网络地址资源和信息资源，可根据实际需要分配地址，避免不必要的地址空间的浪费；
- 地址分配应简单、易于管理，降低网络扩展的复杂性，减少路由表的路由条数；
- 地址分配在每一个层次都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性；
- 地址分配应具有灵活性，以满足各种路由策略的优化，充分利用地址空间；
- 便于制定统一的网络管理策略，实现统一的网络管理；

- 便于网络安全策略的实现；
- 为不同地域间的信息交换设计出优良的稳定网络的 IP 地址编码规范；
- 各局域网内不同类型的应用必须使用不同子网的 IP 地址，以便于不同的应用使用不同的路由策略。

针对 A、B 企业服务器地址段不同，但是用户地址和网络设备地址段重复的现状，可以采用如下的地址切换解决方案，以实现平滑过渡：

- 所有核心设备整合到一个机房后，在服务器区划分三个或多个 VLAN，使原有服务器网段地址不作修改，以保障业务系统的正常使用；
- 用户地址进行统一规划，采用先横向再纵向的方式对各单位进行地址分配，各单位进行地址分配时对地址进行合理预留，以满足后期扩展。并采用 DHCP 技术自动分配业务地址；
- 设备管理地址采用 32 位掩码、属于单一地址段的地址进行全网统一规划，设备互联地址采用 30 位掩码的地址进行全网统一规划。

【问题 3】

OSPF 支持多进程，在同一台路由器上可以运行多个不同的 OSPF 进程，它们之间互不影响，彼此独立。不同 OSPF 进程之间的路由交互相当于不同路由协议之间的路由交互。路由器的一个接口只能属于某一个 OSPF 进程。

本问题是一个较为典型的案例，待整合的网络都采用 OSPF 作为路由协议，只是 OSPF 进程号不同；在进行网络整合的路由规划时，可以采用两种思路：一是在整合后的网络中只存在一个 OSPF 体系，所有路由器都使用相同的 OSPF 进程号；二是所有路由器的原有 OSPF 进程号不发生改变，在整合后的网络中存在两个 OSPF 体系，两个 OSPF 体系之间采用路由引入，使得所有路由器之间可以互访。

参考答案

【问题 1】

解决方案的整体思路：

（1）武汉的核心路由设备迁移到一个核心机房，并迁移原有与二级设备的链路；

（2）所有服务器、核心交换机迁移到武汉的核心机房，并实现服务器区与两台核心交换机的默认网关冗余；

（3）统一采用二级、三级节点方式，打乱原有连接方式；对 8 个二级节点以外的节点都降级为三级节点；对原 A 企业三级节点、B 企业节点分扫描接入点采用就近接入原则或者就近线路迁移原则，形成三级网络结构；

（4）原有 155M 线路作主用，30M 线路作备用。

【问题 2】

地址切换解决方案：

（1）所有核心设备整合到一个机房后，在服务器区划分三个或多个 VLAN，使原有

服务器网段地址不作修改，以保障业务系统的正常使用。

（2）用户地址进行统一规划，采用先横向再纵向的方式对各单位进行地址分配，各单位进行地址分配时对地址进行合理预留，以满足后期扩展。并采用 DHCP 技术自动分配业务地址。

（3）设备管理地址采用 32 位掩码、属于单一地址段的地址进行全网统一规划，设备互联地址采用 30 位掩码的地址进行全网统一规划。

【问题 3】

路由整合方案：

路由整合方案一：整合所有路由器到一个 OSPF 体系中，所有核心设备规划到核心区域 AREA 0 中，其他节点按归属划分到不同的区域中。

路由整合方案二：采用多进程 OSPF 技术，将原有两个单位的 OSPF 启用两个不同的进程，再进行路由的相互导入。

路由整合方案比较：

第一种方案较优，能使整个网络中的路由更加清晰，区域的划分更加合理，并能有效地进行路由汇总。

第二种方案通常是网络整合中的过渡性方案，实际上在网络中存在两个路由体系，借助于路由体系之间的路由引入而形成互连互通，因此形成的最短路径并不是真正意义上的最短路径，并且会影响路由收敛效率。

试题三（25 分）

阅读以下关于某企业内部网络系统的叙述，回答问题 1、问题 2 和问题 3。

某企业网络拓扑结构如图 3-1 所示。根据企业要求实现负载均衡和冗余备份，构建无阻塞高性能网络的建设原则，该企业网络采用两台 S7606 万兆骨干路由交换机作为双核心，部门交换机 S2924G 通过光纤分别与两台核心交换机相连，通过防火墙和边界路由器与 Internet 相连。S7606 之间相连的端口均为 Trunk 端口，S7606 与 S2924G 之间相连的端口也均为 Trunk 端口。

部分 PC 的 IP 信息及所属 VLAN 如表 3-1 所示。

表 3-1　部分 PC 的 IP 信息及所属 VLAN

网络设备	IP 地址	所属 VLAN
PC1	202.10.9.10/24	VLAN 9
PC2	202.10.10.10/24	VLAN 10
PC3	202.10.11.10/24	VLAN 11
PC4	202.10.12.10/24	VLAN 12
PC5	202.10.9.15/24	VLAN 9

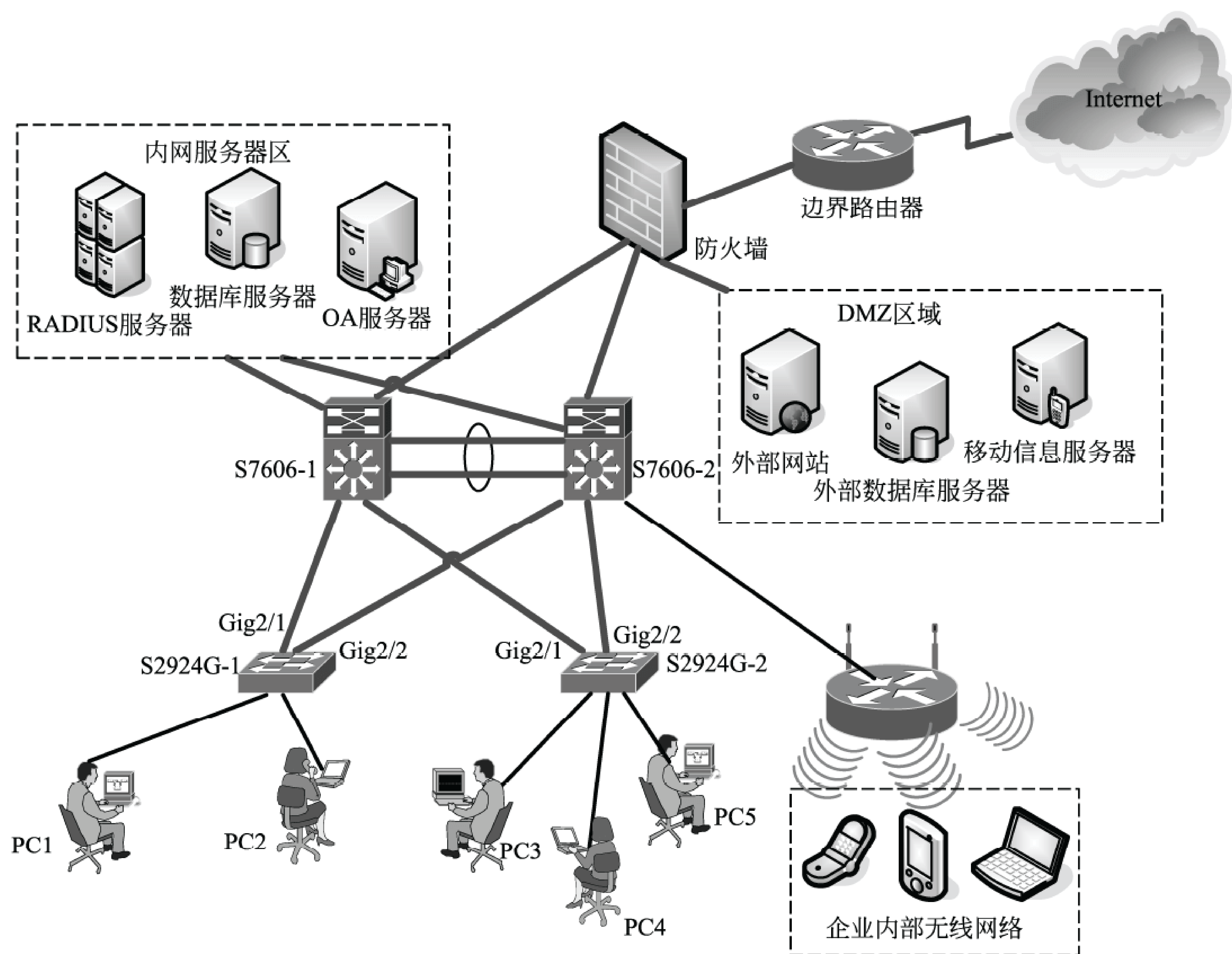


图 3-1　某企业网络拓扑结构

【问题 1】

4 台交换机都启用了 MSTP 生成树模式，其中 S7606-1 的相关配置如下：

```
S7606-1 (config)#spanning-tree mst 1 priority 4096 //缺省值是32768
S7606-1 (config)#spanning-tree mst configuration
S7606-1 (config-mst)#instance 1 vlan 10,12
S7606-1 (config-mst)#instance 2 vlan 9,11
S7606-1 (config-mst)#name region1
S7606-1 (config-mst)#revision 1
```

S7606-2 的相关配置如下：

```
S7606-2 (config)#spanning-tree mst 2 priority 4096
S7606-2 (config)#spanning-tree mst configuration
S7606-2 (config-mst)#instance 1 vlan 10,12
S7606-2 (config-mst)#instance 2 vlan 9,11
```

```
S7606-2 (config-mst)#name region1
S7606-2 (config-mst)#revision 1
```

两台 S2924G 交换机也配置了相同的实例、域名称和版本修订号。

（1）请问 instance 2 的生成树的根交换机是哪一台？为什么？

（2）就 instance 1 而言，交换机 S2924G-1 的根端口是哪个端口？为什么？

（3）请指出 PC1 发给 PC5 的数据包经过的设备路径。

【问题 2】

在三层交换机 S7606-1 中 VLAN 10 的 IP 地址配置为 202.10.10.1/24，VLAN 11 的 IP 地址配置为 202.10.11.254/24。

在三层交换机 S7606-2 中 VLAN 10 的 IP 地址配置为 202.10.10.254/24，VLAN 11 的 IP 地址配置为 202.10.11.1/24。两台三层交换机中的 VRRP 配置如下：

```
S7606-1 (config)# interface Vlan 10
S7606-1 (config-if)# vrrp 10 ip 202.10.10.1
S7606-1 (config-if)# vrrp 10 preempt
S7606-1 (config)# interface Vlan 11
S7606-1 (config-if)# vrrp 11 ip 202.10.11.1

S7606-2 (config)# interface Vlan 10
S7606-2 (config-if)# vrrp 10 ip 202.10.10.1
S7606-2 (config)# interface Vlan 11
S7606-2 (config-if)# vrrp 11 ip 202.10.11.1
S7606-2 (config-if)# vrrp 11 preempt
```

（1）PC2 主机中设置的网关 IP 为 202.10.10.1，在网络正常运行的情况下，请按照以下格式写出 PC2 访问 Internet 的数据转发路径。（格式：PC2→设备 1→…→Internet。不写返回路径）

（2）假设三层交换机 S7606-1 需要临时宕机 1 小时进行检修及升级操作系统。

请问这 1 小时时段内 PC2 在没有修改网关 IP 地址的情况下，是否能访问 Internet？请结合交换机 S7606-1 宕机后发生的变化说明原因。

【问题 3】

企业内部架设有无线局域网，并采用了 802.1X 认证，用户名和密码存放在 Radius 服务器的数据库中。无线路由器 Wirelessrouter1 支持 802.1x 协议，请回答以下问题：

（1）在图 3-2 所示的认证过程中，客户端向无线路由器发送的是什么帧？无线路由器向 Radius 服务器发送的是什么报文？

（2）在无线路由器中需要配置哪些与 Radius 服务器相关的信息？

（3）如果无线路由器不支持 802.1X 认证，为满足无线用户必须经过认证才能上网的需求，能否在上层交换机中启用 802.1X，并将端口设置为启用 dot1x 认证？请简要说

明理由。

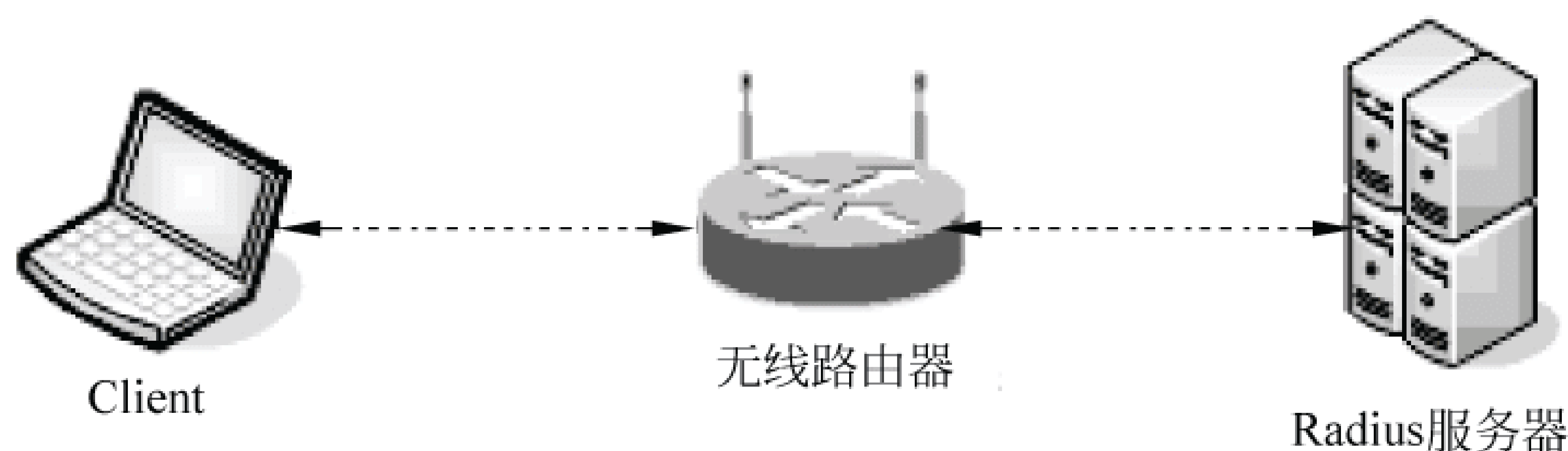


图 3-2　802.1x 认证示意图

试题三分析

本题主要考查 STP、MSTP 和 PVST/PVST+相关知识点。MSTP（Multiple Spanning Tree Protocol，多生成树协议）将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。MSTP 兼容 STP 和 RSTP，并且可以弥补 STP 和 RSTP 的缺陷。它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台交换机以及它们之间的网段构成。这些交换机都启动了 MSTP、具有相同的域名、相同的 VLAN 到生成树映射配置和相同的 MSTP 修订级别配置，并且物理上有链路连通。

一个交换网络可以存在多个 MST 域。用户可以通过 MSTP 配置命令把多台交换机划分在同一个 MST 域内。域内所有交换机都有相同的 MST 域配置：域名相同 *region1*，VLAN 与生成树的映射关系相同（VLAN 10 和 VLAN 12 映射到生成树实例 1，VLAN 9 和 VLAN 11 映射到生成树实例 2）。

【问题 1】

在本问题中，配置 S7606-1 交换机在 instance 1 中的优先级为 4096，缺省是 32768，值越小越优先成为该 instance 中的根交换机。同理，instance 2 的生成树的根交换机是 S7606-2，因为其优先级的值较小，优先成为该实例的根交换机。

对 instance 1 而言，交换机 S2924G-1 的根端口是 Gig2/1 端口，因为 instance 1 的生成树的根交换机是 S7606-1，交换机 S2924G-1 离根桥最近的端口为根端口。

PC1 和 PC5 都属于 VLAN 9，同时 VLAN 9 被映射到实例 2，由于实例 2 生成树的根交换机是 S7606-2，根据生成树算法，对实例 2 而言，S2924G-1 的根端口是 Gig2/2，S2924G-2 的根端口也是 Gig2/2。因此 PC1 到 PC5 的传输路径是：

PC1→S2924G-1（Gig2/2）→S7606-2→S2924G-2（Gig2/2）→PC5

MSTP 与 PVST/PVST+之间的区别：

每个 VLAN 都生成一棵树是一种比较直接而且最简单的解决方法。它能够保证每一

个 VLAN 都不存在环路。但是由于种种原因，以这种方式工作的生成树协议并没有形成标准，而是各个厂商各有一套，尤其是以 Cisco 的 VLAN 生成树 PVST（Per VLAN Spanning Tree）为代表。

为了携带更多的信息，PVST BPDU 的格式和 STP/RSTP BPDU 格式已经不一样，发送的目的地址也改成了 Cisco 保留地址 01-00-0C-CC-CC-CD，而且在 VLAN Trunk 的情况下 PVST BPDU 被打上了 802.1Q VLAN 标签。所以，PVST 协议并不兼容 STP/RSTP 协议。

Cisco 很快又推出了经过改进的 PVST＋协议，并成为其交换机产品的默认生成树协议。经过改进的 PVST+协议在 VLAN 1 上运行的是普通 STP 协议，在其他 VLAN 上运行 PVST 协议。PVST+协议可以与 STP/RSTP 互通，在 VLAN 1 上生成树状态按照 STP 协议计算。在其他 VLAN 上，普通交换机只会把 PVST BPDU 当作多播报文按照 VLAN 号进行转发。但这并不影响环路的消除，只是 VLAN 1 和其他 VLAN 的根桥状态可能不一致。由于每个 VLAN 都有一棵独立的生成树，单生成树的种种缺陷都被克服了。同时，PVST 带来了新的好处，那就是二层负载均衡。

PVST/PVST+协议也有它的明显不足：（1）由于每个 VLAN 都需要生成一棵树，PVST BPDU 的通信量将正比于 Trunk 的 VLAN 个数。（2）当 VLAN 个数比较多时，维护多棵生成树的计算量和资源占用量将急剧增长。特别是当 Trunk 了很多 VLAN 的接口状态发生变化的时候，所有生成树的状态都要重新计算，CPU 将不堪重负。（3）由于协议的私有性，PVST/PVST+不能像 STP/RSTP 一样得到广泛的支持，不同厂家的设备并不能在这种模式下直接互通。

多生成树协议 MSTP（Multiple Spanning Tree Protocol）是 IEEE 802.1s 中定义的一种新型多实例化生成树协议。MSTP 协议的精妙之处在于把支持 MSTP 的交换机和不支持 MSTP 的交换机划分成不同的区域，分别称作 MST 域和 SST 域。在 MST 域内部运行多实例化的生成树，在 MST 域的边缘运行 RSTP 兼容的内部生成树 IST（Internal Spanning Tree）。

MSTP 定义了“实例”（Instance）和域的概念。简单地说，STP/RSTP 是基于端口的，PVST/PVST+是基于 VLAN 的，而 MSTP 就是基于实例的。所谓实例就是多个 VLAN 的一个集合，通过将多个 VLAN 捆绑到一个实例可以节省通信开销和资源占用率。

MSTP 带来的好处是显而易见的。它既有 PVST 的 VLAN 认知能力和负载均衡能力，又拥有可以和 SST 媲美的低 CPU 占用率。

【问题 2】

本问题主要考查 VRRP 相关知识点。

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种容错协议。通常，一个网络内的所有主机都设置一条缺省路由，这样，当主机发出数据包的目的地址不在本网段时，报文将被通过缺省路由发往网关路由器，从而实现了主机与外部网络

的通信。当某网络的默认网关（路由器）坏掉时，本网段内的所有主机将不能与外部网络通信。VRRP 就是为解决这一严重问题而提出的，它为具有多播或广播能力的局域网设计。VRRP 将局域网的一组路由器（包括一个 Master 即主控路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器，称之为一个备份组。

在 VRRP 协议中，有两组重要的概念：VRRP 路由器和虚拟路由器，以及主控路由器和备份路由器。VRRP 路由器是指运行 VRRP 的路由器，是物理实体，虚拟路由器是 VRRP 协议创建的，是逻辑概念。一组 VRRP 路由器协同工作，共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色：主控路由器和备份路由器，一个 VRRP 组中有且只有一台处于主控角色的路由器，可以有一个或者多个处于备份角色的路由器。VRRP 协议使用选择策略从路由器组中选出一台作为主控，负责 ARP 响应和转发 IP 数据包，组中的其他路由器作为备份的角色处于待命状态。当由于某种原因主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主路由器。由于此切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对终端使用者系统是透明的。

一个 VRRP 路由器有唯一的标识：VRID，范围为 0～255。该路由器对外表现为唯一的虚拟 MAC 地址，地址的格式为 00-00-5E-00-01-[VRID]。主控路由器负责对 ARP 请求用该 MAC 地址做应答。这样，无论如何切换，保证给终端设备的是唯一一致的 IP 和 MAC 地址，减少了切换对终端设备的影响。

VRRP 控制报文只有一种：VRRP 通告（advertisement）。它使用 IP 多播数据包进行封装，组地址为 224.0.0.18，发布范围只限于同一局域网内。这保证了 VRID 在不同网络中可以重复使用。为了减少网络带宽消耗，只有主控路由器才可以周期性地发送 VRRP 通告报文。备份路由器在连续三个通告间隔内收不到 VRRP 或收到优先级为 0 的通告后启动新的一轮 VRRP 选举。

在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中优先级范围是 0～255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器作 VRRP 组中的 IP 地址所有者；IP 地址所有者自动具有最高优先级：255。优先级 0 一般用在 IP 地址所有者主动放弃主控者角色时使用。可配置的优先级范围为 1～254。优先级的配置原则可以依据链路的速度和成本、路由器性能和可靠性以及其他管理策略设定。主控路由器的选举中，高优先级的虚拟路由器获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。对于相同优先级的候选路由器，按照 IP 地址大小顺序选举。VRRP 还提供了优先级抢占策略，如果配置了该策略，高优先级的备份路由器便会剥夺当前低优先级的主控路由器而成为新的主控路由器。

为了保证 VRRP 协议的安全性，提供了两种安全认证措施：明文认证和 IP 头认证。明文认证方式要求：在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。适合于避免在局域网内的配置错误，但不能防止通过网络监听方式获得密码。IP

头认证的方式提供了更高的安全性，能够防止报文重放和修改等攻击。

在本小题中，在两台 S7606 中都配置了两个虚拟备份组，虚拟备份组 10 的 IP 地址为 202.10.10.1/24;虚拟备份组 11 的 IP 地址为 202.10.11.1/24。虚拟备份组 10 为 VLAN 10 中的主机提供了网关冗余，虚拟备份组 11 为 VLAN 11 中的主机提供了网关冗余。

由于 VRRP 路由器 S7606-1 的 IP 地址和虚拟备份组 10 的 IP 地址相同，因此其具有最高优先级，成为虚拟备份组 10 的主控路由器，S7606-1 为虚拟组 10 的备份路由器。

在网络正常运行的情况下，主机 PC2 访问 Internet 的数据转发路径为：

PC2→S2924G-1→S7606-1→防火墙→边界路由器→Internet。

当路由器 S7606-1 宕机后，PC2 不用修改网关 IP 地址，就可以访问 Internet。因为当虚拟备份组 10 的备份路由器 S7606-2 在数秒之内没有收到主控路由器的通告，会认为主控路由器失效，就会自动启动切换，成为主控路由器，响应对虚拟 IP 地址的 ARP 请求，并且响应的是虚拟 MAC 地址，而不是接口的真实 MAC 地址。同时负责转发目的 MAC 地址为虚拟 MAC 地址的 IP 报文，这样就保证了对客户透明的网关切换。

【问题 3】

IEEE 802.1x 是根据用户 ID 或设备，对网络客户端（或端口）进行鉴权的标准。该流程被称为“端口级别的鉴权”。它采用 RADIUS（远程认证拨号用户服务）方法，并将其划分为三个不同的小组：请求方、认证方和授权服务器。802.1x 标准应用于试图连接到端口或其他设备（如 Cisco Catalyst 交换机或 Cisco Aironet 系列接入点）（认证方）的终端设备和用户（请求方）。认证和授权都通过鉴权服务器（如 Cisco Secure ACS）后端通信实现。IEEE 802.1x 提供自动用户身份识别，集中进行鉴权、密钥管理和 LAN 连接配置。整个 802.1x 的实现设计三个部分：请求者系统、认证系统和认证服务器系统。

请求者是位于局域网链路一端的实体，由连接到该链路另一端的认证系统对其进行认证。请求者通常是支持 802.1x 认证的用户终端设备，用户通过启动客户端软件发起 802.1x 认证。认证系统对连接到链路对端的认证请求者进行认证。认证系统通常为支持 802.1x 协议的网络设备，它为请求者提供服务端口，该端口可以是物理端口，也可以是逻辑端口，一般在用户接入设备 （如 LAN Switch 和 AP）上实现 802.1x 认证。请求者和认证系统之间运行 802.1x 定义的 EAPoL（Extensible Authentication Protocol over LAN）协议。当认证系统工作于中继方式时，认证系统与认证服务器之间运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其他高层次协议中（如 RADIUS），以便穿越复杂的网络到达认证服务器；当认证系统工作于终结方式时，认证系统终结 EAPoL 消息，并转换为其他认证协议（如 RADIUS），传递用户认证信息给认证服务器系统。认证系统每个物理端口内部包含有受控端口和非受控端口。非受控端口始终处于双向连通状态，主要用来传递 EAPoL 协议帧，可随时保证接收认证请求者发出的 EAPoL 认证报文；受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

在无线路由器中需要配置的 Radius Server 信息有：IP 地址、认证和授权端口（只写

端口也可以）、与 RADIUS 服务器一致的密钥。

RADIUS 是 Remote Authentication Dial-In User Service（远程认证拨号用户服务）的简称，作为一种分布式的客户机/服务器系统，能提供 AAA 功能。RADIUS 技术可以保护网络不受未授权访问的干扰，常被用在既要求较高安全性、又要求维持远程用户访问的各种网络环境中（如用来管理使用串口和调制解调器的大量分散拨号用户）。

RADIUS 服务包括三个组成部分：

（1）协议：rfc2865、2866 协议基于 udp/ip 层定义了 RADIUS 帧格式及消息传输机制，并定义了 1812 作为认证端口，1813 作为计费端口。（2）服务器：RADIUS 服务器运行在中心计算机或工作站上，包含了相关的用户认证和网络服务访问信息。（3）客户端：位于拨号访问服务器 NAS（Network Access Server）侧，可以遍布整个网络。

RADIUS 基于客户/服务器模型，NAS（如路由器）作为 RADIUS 客户端，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理（如接入/挂断用户）。RADIUS 服务器负责接收用户连接请求，认证用户，然后给 NAS 返回所有需要的信息。RADIUS 服务器对用户的认证过程通常需要利用 NAS 等设备的代理认证功能，RADIUS 客户端和 RADIUS 服务器之间通过共享密钥认证相互间交互的消息，用户密码采用密文方式在网络上传输，增强了安全性。RADIUS 协议合并了认证和授权过程，即响应报文中携带了授权信息。

题中无线路由器即为 NAS，要使得它能与 RADIUS 服务器正常通信，根据上述原理，在无线路由器中需要配置 RADIUS 服务器的 IP 地址、认证和授权端口、与 RADIUS 服务器一致的密钥。

如果无线路由器不支持 802.1 x 认证，只要在上层交换机中启用 802.1x，并将端口设置为启用 dot1x 认证，就可以达到通过 RADIUS 服务器进行验证的功能。这种方式有两种认证模式：port-based 和 mac-based。port-based 模式下，只要物理端口下的第一个用户认证成功后，其他接入该端口的用户无需认证就可以访问网络资源，当第一个用户下线后，端口被“关闭”，其他用户也会被阻止访问网络。而在 mac-based 模式下，接入物理端口的所有主机都需要进行认证才能访问网络资源，当某用户下线时，将不影响其他用户的认证状态，其他用户还可以继续访问网络。如果端口通过交换机接入了多台主机，那么为了使每台主机都要进行认证，应使用此认证模式。

参考答案

【问题 1】

（1）instance 2 的生成树的根交换机是 S7606-2，因为其优先级的值较小，优先成为该实例的根交换机。（2 分）

（2）对 instance 1 而言，交换机 S2924G-1 的根端口是 Gig2/1 端口，因为 instance 1 的生成树的根交换机是 S7606-1，交换机 S2924G-1 离根桥最近的端口为根端口。（2 分）

（3）PC1→S2924G-1→S7606-2→S2924G-2→PC5（2 分）

（4）PVST/PVST+是 Cisco 公司提出的生成树协议，核心思想是为每个 VLAN 都计算一个生成树，这样可以在具有链路冗余保护的情况下，实现第二层的负载均衡。PVST/PVST+存在的问题是：由于每个 VLAN 都需要维护一个生成树，BPDU 的通信量较大；当 VLAN 个数较多的时候，维护多棵生成树的计算量和资源占用量将急剧增长；属于私有协议。（3 分）

【问题 2】

（1）在网络正常运行的情况下，PC2 访问 Internet 的数据转发路径为：

PC2→S2924G-1→S7606-1→防火墙→边界路由器→Internet（2 分）

（2）能访问 Internet。（2 分）

（3）虚拟路由冗余协议 VRRP 是用于实现路由器冗余的协议，对共享多存取访问介质（如以太网）上终端 IP 设备的默认网关（Default Gateway）进行冗余备份，从而在其中一台路由设备宕机时，备份路由设备及时接管转发工作，向用户提供透明的切换，提高了网络服务质量。

根据给出的配置可知，在网络正常情况下，VRRP 组 10 的主控路由器是 S7606-1，备份路由器是 S7606-2。当交换机 S7606-1 宕机后，经过主路由器失效间隔时间后，备份路由器会自动切换为主控路由器，整个过程对用户是透明的，因此客户机并不需要修改网关 IP，仍可以连接 Internet。（4 分）

【问题 3】

（1）客户端向无线路由器发送的是 EAPoL（Extensible Authentication Protocol over LAN）帧；无线路由器向 RADIUS 服务器发送的是 EAP over RADIUS 报文，因为认证系统将 EAP 帧封装到 RADIUS 报文中发送给认证服务器。（2 分）

（2）在无线路由器中需要配置的 RADIUS Server 信息有：IP 地址、认证和授权端口（只写端口也可以）与 RADIUS 服务器一致的密钥。（3 分）

（3）如果无线路由器不支持 802.1x 认证，可以在上层交换机中启用 802.1x，并将端口设置为启用 dot1x 认证。但注意上层交换机下联无线路由器的 802.1x 端口认证模式应设置为 mac-based。这样接入物理端口的所有主机都需要进行认证才能访问网络资源。当某用户下线时，将不影响其他用户的认证状态，其他用户还可以继续访问网络。（3 分）

第 9 章　2010 下半年网络规划设计师下午试卷 II 写作要点

论题一　论校园网/企业网的网络规划与设计

校园网（或企业网）是计算机网络的一大分支，有着非常广泛的应用及代表性。对于校园网/企业网，完备的应用是关键，而稳定可靠的网络是基础，完善的安全和管理手段是保障。由于学校/企业的类型和规模的不同，校园网/企业网的规划设计有着多种解决方案。校园网的规划、设计、硬件建设、软件建设以及网络的使用、扩充等都要从全局、长远的角度出发，充分考虑网络的安全性、易用性、可靠性和经济性等。

请围绕“校园网/企业网的网络规划与设计”论题，依次对以下三个方面进行论述。

1. 概要叙述你参与设计实施的网络项目以及你所担任的主要工作。

2. 具体讨论在校园网/企业网网络规划与设计中的主要工作内容和你所采用的原则、方法和策略，以及遇到的问题和解决措施。

3. 分析你所规划和设计的校园网/企业网网络的实际运行效果。你现在认为应该做哪些方面的改进以及如何加以改进。

写作要点

1．叙述自己参与设计和实施的校园网/企业网网络项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量。

2．能够全面和准确地描述该校园网/企业网网络的应用环境和需求，深入地阐述采用了哪些技术和方法，这些技术和方法要针对校园网/企业网网络的特点，具有一定的广度和深度。

3．对需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

论题二　论网络规划与设计中新技术的使用

随着计算机技术和通信技术的迅猛发展，计算机网络技术的发展也可用日新月异来形容。在计算机网络的交换技术、网络安全技术、光通信技术、无线通信技术、网络存储技术等诸多方面不断地涌现出各种新技术。在网络规划和设计中，如何根据项目的现状和实际需求，积极地引进和使用新技术，是网络规划设计师的职责。

请围绕“网络规划中新技术的使用”论题，依次对以下三个方面进行论述。

1. 概要叙述你参与设计和实施的网络应用项目以及你所担任的主要工作。

2. 具体阐述你在网络规划与设计中采用了哪些新技术和新方法，使用这些新技术和新方法的应用背景、需求和目的是什么？

3. 分析你使用上述新技术、新方法的效果如何，以及相关的改进措施。

写作要点

1．叙述自己参与设计和实施的网络应用项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量。

2．能够全面和准确地描述采用新技术和新方法的应用背景、需求和目的，深入地阐述采用了哪些新技术和新方法，这些技术和方法要符合应用背景和需求，具有一定的广度和深度，而不是堆砌技术。

3．对需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

第 10 章　2011 下半年网络规划设计师上午试题分析与解答

试题（1）

（1）传递需要调制编码。

A. 数字数据在数字信道上　　B. 数字数据在模拟信道上

C. 模拟数据在数字信道上　　D. 模拟数据在模拟信道上

试题（1）分析

本题考查数字传输与模拟传输和模拟数据和数字数据调制的基本概念。

按承载信息的电信号形式不同，通信可分为模拟传输和数字传输。模拟传输是以模拟信号来传输消息的通信方式，在模拟信道上传输；数字传输是指用数字信号来传送消息的方式，在数字通道上传输。数字数据在数字信道上传输需要将其转变为数字信号，采用相应的数字编码；数字数据在模拟信道上传输需要调制成模拟信号；模拟数据在数字信道上传输时，需要将其通过量化编码转成数字信号；模拟数据在模拟信道上传输时，可以进行调制也可以不进行调制传输。

参考答案

（1）B

试题（2）

某一基带系统，若传输的比特数不变，而将二电平传输改为八电平传输，如 T2 和 T8 分别表示二电平和八电平码元间隔，则它们的关系是（2）。

（2）　A. T8=3T2　　B. T8=2T2　　C. T8=8T2　　D. T8=4T2

试题（2）分析

本题考查数据通信的基本概念。

数据通信系统传输的有效程度可以用码元传输速率和信息传输速率来描述。码元传输速率表示单位时间内数据通信系统所传输的码元个数，这里的码元可以是二进制，也可以是多进制的。信息传输速率又可称为信息速率、比特率等，表示单位时间内数据通信系统所传输的二进制码元个数。在 M 电平传输系统中，信息速率 Rb 和码元率 Rs 之间的关系为：

$Rb=Rs\log_2 M$

数据通信系统传输中，若传输的比特数不变，传输电平数增加，传输周期就要展宽。本题中，Rb=3Rs，所以 T8=3T2。

参考答案

（2）A

试题（3）

偶校验码为 0 时，分组中“1”的个数为__（3）__。

（3）A. 偶数　　B. 奇数　　C. 未知数　　D. 以上都不对

试题（3）分析

本题考查数据通信检错和纠错基本知识。

在数据传输过程中，由于信道受到噪声和干扰的影响，可能会出现传输错误，通过在发送的信息后加冗余位来进行差错控制。寄偶校验码是一种最简单的校验码，其编码规则：先将所要传送的数据码元分组，并在每组的数据后面附加一位冗余位即校验位，使该组包括冗余位在内的数据码元中“1”的个数保持为奇数（奇校验）或偶数（偶校验）。在接收端按照同样的规则检查，如发现不符，说明有错误发生。

参考答案

（3）A

试题（4）

用户在开始通信前，必须申请建立一条从发送端到接收端的物理信道，并且在双方通信期间始终占用该信道，这样的交换方式属于__（4）__。

（4）A. 电路交换　　B. 报文交换　　C. 分组交换　　D. 信元交换

试题（4）分析

本题考查数据通信的交换方式的概念。

两个终端开始正式通信之前，首先由主呼终端进行呼叫，送出被呼终端的电话号码，直到在主呼和被呼之间建立起一条专用的通信线路，主呼终端和被呼终端才开始进行双向数据传输，在整个数据传输期间一直独占线路，通信结束后释放已建立的通信线路，这种技术叫做电路交换或是线路交换，主要用于电话系统。

发送方待发送的整个数据块称为报文（message）。报文交换事先不建立线路，当发送方有数据块要发送时，它把目的地址附加在报文上交给交换设备，交换设备选择一条合适的空闲输出线，将报文通过该输出线传送出去。在这个过程中，交换设备的输入线和输出线之间不建立物理连接，在每个交换设备处，报文首先被存储起来，在适当的时候被转发出去，所以报文交换采用的是存储转发技术，动态分配线路，使得线路能够共享，提高了资源的利用率。

为了解决报文交换大报文传输的问题，分组交换技术严格限制数据块大小的上限，把大报文切分成更小的数据单位，加上一些必要的控制信息组成的首部后，就构成了分组（packet），分组从发送端发出，经过一个或多个交换设备转发，转发的选路根据分组的首部信息进行，到达接收端，分组可以在交换设备的内存中缓存，同时保证任何用户都不能独占线路超过几十毫秒，现代网络绝大多数采用分组交换技术。分组交换网由若干个交换机和连接这些交换机的链路组成，每台主机都有一条到交换机的链路，交换机的主要工作就是在它的一条链路上接收输入分组，把这些分组从其他的链路上输出。

信元交换是异步传输模式（Asynchronous Transfer Mode，ATM）采用的交换方式，在很大程度上就是按照虚电路方式进行分组转发。在 ATM 网络中与众不同的一点是，分组长度是固定不变的，称为信元（cell）。信元长度为 53 字节，5 字节的首部，48 字节的有效载荷。

参考答案

（4）A

试题（5）

在数字通信中，使收发双方在时间基准上保持一致的技术是 （5） 。

（5） A．交换技术　　B. 同步技术　　C. 编码技术　　D. 传输技术

试题（5）分析

本题考查数据通信的同步方式的概念。

同步控制的方法包括异步起止方式和同步方式。在异步起止方式中，接收方和发送方各自内部有时钟发生器，但频率必须一致。通信双方进行异步串行通信必须遵守异步串行通信控制规程，其特点是通信双方以字符作为数据传输单位，且发送方传送字符的间隔时间是不定的。在同步串行通信方式中，以某种方式将发送方的时钟信号也发送过去，接收方用这个统一的时钟信号来选通数据信号，以此得到和发送完全一致的结果。由于同步串行通信发送端和接收端具有统一的时钟信号，发送和接收的每一位信号都受同步信号的调整，因此，同步串行通信一次传送的信息量比异步串行通信大得多，但是付出的代价是设备复杂。

参考答案

（5）B

试题（6）

在 OSI 参考模型中能实现路由选择、拥塞控制与互连功能的层是 （6） 。

（6）A. 传输层　　B. 应用层　　C. 网络层　　D. 物理层

试题（6）分析

本题考查计算机网络的网络体系结构。

计算机网络是一个复杂的系统，通常把计算机网络按照一定的功能与逻辑关系划分成一种层次结构，OSI 参考模型是计算机网络的基本体系结构模型，OSI 共分为七层，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

物理层为建立、维持与拆除数据链路实体之间二进制位流传输的物理连接，提供机械的、电气的、功能的和规程的特性。物理连接可以通过中继系统，允许进行全双工或半双工的二进制位流的传输。物理层的数据服务单元是比特，它可以通过同步或异步的方式进行传输。

数据链路层是 OSI 模型的第 2 层，它介于物理层与网络层之间。用于在相邻结点间建立数据链路，传送以帧为单位的数据，使其能够有效、可靠地进行数据交换。本层通

过差错控制、流量控制等，将不可靠的物理传输信道变成无差错的可靠的数据路。将数据组成适合正确传输的帧形式的数据单元，对网络层屏蔽物理层的特性和差异，使高层协议不必考虑物理传输介质的可靠性问题，而把信道变成无差错的理想信道。

网络层是通信子网的最高层，是高层与低层协议之间的界面层。网络层用于控制通信子网的操作，是通信子网与资源子网的接口。网络层关系到通信子网的运行控制，决定了资源子网访问通信子网的方式。

设置网络层的主要目的就是为报文分组以最佳路径通过通信子网到达目的主机提供服务，而网络用户不必关心网络的拓扑结构与使用的通信介质。网络层的主要功能如下。

（1）网络连接功能：网络层实体作为数据链路层服务用户，利用各条链路上的数据链路连接服务，来为传送实体之间建立端到端的网络连接关系。其中，涉及到数据通路的建立、维护和拆除的过程。

（2）路由选择功能：路由选择是为建立数据通路服务的一种功能。也就是为在源/宿结点之间建立通路而提供一些控制的过程。这些控制过程由路由算法来实现。

（3）拥塞控制功能：拥塞控制的主要功能是对进入网络的数据流实施有效控制，使通信子网避免发生“网络拥塞”和“死锁”现象，保持稳定运行。

（4）数据传输功能：在网络连接建立之后，网络层实体要为上层递交下来的数据提供传输与中继功能。根据通路的类型，传送服务数据可能在一个子网内进行，也可能要跨越互连设备进行中继转发。传输过程包括对数据的分组、排序以及进行差错和速度控制等。

（5）其他功能：除了具有以上功能外，网络层还提供诸如子网接入、网络连接复用、计费以及在网络互连环境下的协议转换等功能。

传输层是网络体系结构中最关键的一层，是资源子网和通信子网的界面与桥梁，它是面向应用的高层和面向通信的低三层协议之间的接口。传输层主要具有以下功能。

（1）连接管理：传输层连接的管理包括端到端连接的建立、维持和拆除。传输层可同时支持多个进程的连接，即将多个进程连接复用在一个网络层连接上。

（2）优化网络层提供的服务质量：传输层优化网络服务质量包括检查低层未发现的错误、纠正低层检测出来的错误、对接收到的数据包重新排序、提高通信可用带宽、防止无访问权的第三者对传输的数据进行读取或修改等。

（3）提供端到端的透明数据传输：传输层可以弥补低层网络所提供服务的差异，屏蔽低层网络的细节操作，对数据传输的控制包括数据报文分段和重组、端到端差错检测和恢复、顺序控制和流量控制等。

（4）多路复用和分流：当传输层用户进程的信息量较少时，将多个传输连接映射到一个网络连接上，以便充分利用网络连接的传输速率，减少网络连接个数。

应用层功能网络的应用层是网络体系结构中的最高层，它是计算机开放互连环境与

本地系统的操作环境和应用系统直接接口的一个层次。在功能上，应用层为本地系统的应用进程（Application Process）访问网络环境提供手段，也是唯一直接给应用进程提供各种应用服务的层次。即借助应用实体、应用协议和应用服务实现端点用户之间的信息交换。

参考答案

（6）C

试题（7）

HDLC 协议采用的帧同步方法为__（7）__。

（7）A. 字节计数法　　B. 使用字符填充的首尾定界法

C. 使用比特填充的首尾定界法　　D. 其他编码法

试题（7）分析

本题考查数据链路层协议 HDLC 的基本概念。

数据链路层协议中最有代表性的是高级数据链路控制协议（HDLC）。HDLC 是面向比特的数据链路控制规程，HDLC 协议具有透明传输、可靠性高、传输效率高和灵活性强等特点。HDLC 协议规定了数据传输的操作模式、数据帧格式、帧类型等。

所有的帧都使用下列标准的帧格式，包括链路控制信息和数据。链路控制信息包括帧首和帧尾的标志序列 F、地址字段 A、控制字段 C、帧校验序列 FCS 。HDLC 协议规定了长格式和短格式两种帧。长格式包括数据信息字段 I 和链路控制信息，短格式只包含链路控制信息。

F	A	C	I	FCS	F

HDLC 帧格式

标志序列 F：是一个独特的 8 位序列（01111110），表示帧的开始和结束。它也可兼作上一个帧的结束标志和下一个帧的开始标志，具有帧同步的作用。标志序列也可用作帧间填充。不包括标志序列在内，如果一个帧的长度小于 32 位，则认为该帧无效。

地址字段 A：在命令帧中，给出执行该命令的次站地址，响应中给出作出应对的次站地址，地址字段通常为 8 位，允许采用扩充地址字段。具体办法是：保留每个 8 位地址的最低位为 0 来表示后面跟着的 8 位是该基本地址的扩充地址，扩充地址的格式与基本地址相同，依次采用上述方法可以多次对地址字段进行扩充。

控制字段 C：用于表示所使用帧的类型以及序列号。该字段也可以被用来去命令被选站执行某种操作，或传递被选站对主站命令的应答。

信息字段 I：表示链路所要传输的实际信息。

帧校验序列 FCS：可以使用 16 位或 32 位的帧校验序列，用于差错检测。

参考答案

（7）C

试题（8）

下列哪个协议是无线局域网通信协议__（8）__。

（8）A. IEEE 1394　B. IEEE 802.1x　C. IEEE 802.11　D. IEEE 802.13

试题（8）分析

本题考查有关局域网标准的基本概念。

1980 年 2 月 IEEE 成立 IEEE 802 委员会，负责制定局域网标准。IEEE 802 委员会制定一系列标准，主要包括：

IEEE 802.1A：局域网概述及体系结构。

IEEE 802.1B：寻址、网络互连与网络管理。

IEEE 802.2：逻辑链路控制（LLC）。

IEEE 802.3：以太网的 CSMA/CD 总线访问控制方法与物理层规范。

IEEE 802.4：令牌总线（Token Bus）访问控制方法与物理层规范。

IEEE 802.5：令牌环访问控制方法与物理层规范。

IEEE 802.6：城域网（MAN）访问控制方法与物理层规范。

IEEE 802.7：宽带局域网访问控制方法与物理层规范。

IEEE 802.8：FDDI 访问控制方法与物理层规范。

IEEE 802.9：综合语音和数据的访问方法和物理层规范。

IEEE 802.10：网络安全与加密访问方法和物理层规范。

IEEE 802.11：无线局域网访问控制方法与物理层规范。

IEEE 802.12：100VG-AnyLAN 快速局域网访问控制方法与物理层规范。

IEEE 802.14：利用有线电视（Cable-TV）的宽带通信标准。

IEEE 802.15：无线个人区域网（WPAN）规范。

IEEE 802.16：宽带无线网标准。

其中 802.4, 802.5, 802.12 已经淘汰。

参考答案

（8）C

试题（9）

以太网中使用什么机制来检测冲突__（9）__。

（9）A. CDMA/CD　B. 令牌　C. CSMA/CD　D. 探测报文

试题（9）分析

本题考查局域网的访问控制方式的相关知识。

环型局域网利用环接口设备将传输介质连接成环状，计算机连接到环接口设备上。所组成的环可以是单环，也可以是双环。令牌传递访问控制方式应用在环型局域网上。

以太网的核心技术是共享总线的介质访问控制方法（CSMA/CD），用于解决多个结点共享总线的发送权问题。

载波侦听多路访问/冲突检测（CSMA/CD）控制方式原理如下：

① 每个结点在发送数据前，先监听信道，以确定介质上是否有其他结点发送的信号在传送。

② 若介质忙（有信号在传送），则继续监听。

③ 否则，若介质处于空闲状态，则立即发送信息。

④ 在发送过程进行冲突检测。如果发生冲突，则立即停止发送，并向总线上发出一串阻塞信号（全 1）强化冲突，以保证总线上所有结点都知道冲突已发生，转⑤。

⑤ 随机延迟一段时间后返回①。

A、D 两个选项与局域网的访问控制方式无关。

参考答案

（9）C

试题（10）

一个标准的 C 类网络（IPv4 网络）最多可以划分<u>（10）</u>个子网。

（10）A. 128　　B. 256　　C. 32　　D. 64

试题（10）分析

本题考查 IPv4 地址分类和子网划分的有关知识。

（1）IP 地址

在 Internet 上的每一台主机和路由器都分配有一个唯一的 32 位地址，即 IP 地址，也称作网际地址。IP 地址一般采用国际上通行的点分十进制表示。

一个 IP 地址由 4 个字节组成，字节之间用点“.”分隔，每个字节表示为从 0～255 的十进制数（8 位二进制数最大为 11111111，即十进制数 255），这个表示法称为 IP 地址的点分十进制表示法（dotted decimal notation）。

IP 地址由两部分组成：网络号和主机号。网络号标识主机所连接的网络，也叫网络地址；主机号则标识该网络上某个特定的主机，也称主机地址。对一个互联网来说，网络号必须在互联网中唯一，而主机号在该网络内也必须唯一。

一般来说，互联网上的每个接口必须有一个唯一的 IP 地址，因而多接口主机具有多个 IP 地址，其中每个接口都对应一个 IP 地址。

（2）IP 地址分类

IP 协议规定了 IP 地址分为五类，分别是 A、B、C、D、E 类。如下图所示。

0　1　2　3　4　　8　　16　　24　　31

A 类	0		网络号			主机号
B 类	1	0	网络号			主机号
C 类	1	1	0	网络号		主机号
D 类	1	1	1	0	组播（multicast）地址	
E 类	1	1	1	1	保留给将来使用	

IP 地址分类是根据网络号的最高几位来区分，图中的格式规定了用作网络号和主机号的位数，因此也就确定了各类地址的网络总数以及每个网络中主机总数。 A 、B 、C 三类地址可以使用大小不同的网络。

A 类地址的最高位为“0”，其后 7 位是网络号，24 位用作主机号。A 类地址共 126 个网，它用于少数主机数量众多的大型网络，主机数可以 16777216–2 = 16777214。B 类地址的最高 2 位为“10”，其后 14 位为网络号，16 位用作主机号。B 类地址共 16384 个网，它用于中等规模的网络，每个网络主机数最多为 65536–2 = 65534。C 类地址的最高 3 位为“110”，其后 21 位为网络号，8 位用作主机号。C 类地址共 2097152 个网，它用于小型网络，每个网络的主机数只能少于 256–2 = 254。

D 类地址为组播（multicast）地址，它用一个地址代表一组主机。

E 类是实验性地址，保留给将来使用。

在同一个互联网上， IP 地址必须唯一。另外，它还有如下规则：

- A 类地址中以 127 打头的保留作为内部回送地址（loopback），不能用作公共网地址；
- 各比特全 0 和全 1 的网络号和主机号不允许用于分配，用于特殊作用。主机号各比特位全为 0 表示“本地主机”；主机号各位全 1 是代表本网络内所有主机，即网内广播地址，其余的主机号才允许用于分配给网内各主机；网络号为 0 解释为“本网”，网络号全 1 指有限广播网络。

（3）子网和子网划分

A 类网络是很大的一个网络，事实上也没有这样大的网络，因此在实际应用中， IP 地址还可以分层：将一个网络分为多个子网，如可将一个 A 类网络分成 256 个 B 类大小的子网（subnet），同样，B 类地址、C 类地址也可以分层。在分层时，不再把 IP 地址看成由单纯的一个网络号和一个主机号组成，而是把主机号再分成一个子网号和一个主机号。这就是所谓的子网编址（subnet addressing），现在所有的主机都要求支持子网编址。例如一个 B 类网，可以把主机地址中前 8 位用来表示子网地址，后 8 位留作主机地址，这种 B 类网 IP 地址格式如图下图所示。这样就允许有 254 个子网，每个子网可以有 254 台主机。

0	8	16	24　　　31
10	网络号	子网地址	主机地址

同一网络中的不同子网用子网掩码来划分，子网掩码（subnet mask）是网际地址中对应网络标识编码的各位 1，对应主机标识编码的各位为 0 的一个四字节整数，也叫做子网屏蔽码。对于 A、B、C 三类网络来说，它们都有自己默认的掩码，即没有划分子网时的掩码，如下图所示。

屏蔽码示例

类	默认的屏蔽码	高 6 位用做子网地址的屏蔽码
A	255.0.0.0	255.252.0.0
B	255.255.0.0	255.255.252.0.0
C	255.255.255.0	255.255.255.252

子网掩码的作用是：如果两台主机的 IP 地址和子网掩码的“与”的结果相同，则这两台主机是在同一个子网中。

（4）总结

一个标准的 C 类网络有 8 位（8bit）主机 ID，一个最小的子网至少需要 4 个地址（主机 ID 全 0 和全 1 的地址不能用于分配，剩余两个为主机号），因此，一个标准的 C 类网络最多可划分 $2^8÷4=64$ 个子网。

参考答案

（10）D

试题（11）

一个 IP 数据包经过一台路由器转发到另一个网络，该 IP 数据包的头部字段中一定会发生变化的是（11）。

（11）A. 源 IP　　B. 协议号　　C. 目的 IP　　D. TTL

试题（11）分析

本题考查路由器的工作原理和 IP 分组中 TTL 字段的含义。

（1）IP 数据包结构

IP 数据包是 Internet 的基本传送单元，包括数据包包头和数据区两部分。下图表示了 IP 数据包格式。

<table>
<tr><td>0</td><td>4</td><td>8</td><td colspan="3">16</td><td>20</td><td>31</td></tr>
<tr><td>版本</td><td>报头长</td><td>服务类型</td><td colspan="5">总长度</td></tr>
<tr><td colspan="3">标识</td><td></td><td>DF</td><td>MF</td><td colspan="2">分片位移</td></tr>
<tr><td colspan="2">生存时间</td><td>协议号</td><td colspan="5">报头校验和</td></tr>
<tr><td colspan="8">源 IP 地址</td></tr>
<tr><td colspan="8">目的 IP 地址</td></tr>
<tr><td colspan="8">选项＋填充</td></tr>
<tr><td colspan="8">数据</td></tr>
<tr><td colspan="8">…</td></tr>
</table>

IP 数据包格式

IP 协议的数据包头中主要字段如下：

- 版本字段

4bit。用来标识 IP 协议的版本。目前的 IP 协议版本是 4，下一代 IP（IPv6）协议

为 6。

- 包头长度字段

4bit。该字段紧跟在版本号字段后，表示以 32 位（4 个字节）为单位的包头长度。

- 服务类型字段

8bit。指明服务类型或优先级，用于实现区分服务或优先级选路机制。

- 总长度字段

16bit。以字节为单位的 IP 包长度（包含 IP 头在内），IP 包最大长度 65535 字节。

- 标识符与分段偏移量字段

IP 包可能会被分段，这些字段用于分段和到达目的地后的重组。

- 协议字段

协议字段指出用于 IP 数据包携带的高层协议。IP 协议的高层最常用的是 TCP 和 UDP；TCP 的协议代码为 6；UDP 协议代码为 17。

- 源地址和目的地址字段

源地址字段和目的地址字段都是 32 位（32bit）。源地址字段存放发送该 IPv4 数据包的原始 IPv4 地址（数据包会经路由器转发，转发路由器地址不是源地址）；目的地址字段存放最终接收该 IPv4 数据包的设备的 IP 地址（转发路由器也会接收其他路由器转发过来的 IPv4 包，但目的地址并不指向该转发路由器）。

（2）路由器转发原理

从 OSI 七层模型的角度看，路由器是工作在三层（网络层），完成三层协议转发的设备。对 Internet 来说，其三层协议就是 IP 协议，因此 Internet 的路由器可以称为 IP 路由器。

在 Internet 中，路由器用于连接多个逻辑上分开的网络，这些逻辑网络是指一个单独的网络或一个子网，用网络 ID 来标识。当数据从一个子网传输到另一个子网时，必须通过路由器转发来完成。路由器具有判断网络地址和选择路径（路由选择）的功能。

总体而言，Internet 路由器是连接 IP 子网的设备，并在两个或多个不同的 IP 子网之间进行 IP 包的转发。IP 子网由 IP 地址中网络 ID（包括子网 ID）部分来标识，网络 ID 不同即为不同的 IP 子网。

（3）TTL 字段的作用

TTL 是 Time To Live 的缩写，含义为“生存时间”。为避免因错误选路而产生的环路现象（IP 包在一个循环的路由中传递，永远到达不了目的地）。该字段定义了 IP 数据包可存在的最大期限。由于确切的生存时间很难把握，该字段通常用跳跃站点数来度量，即当数据包从一个网络传送到另一个网络时（即经过一个路由器的转发），该字段的值减 1。当该字段为 0 时，数据包将被丢弃。

参考答案

（11）D

试题（12）

假定在一个 IPv4 网络中只有两个主机 HA 和 HB，HA 和 HB 在同一个 LAN 内，并且没有划分 VLAN。如果 HA 和 HB 需要直接通信则需满足（12）。

（12）A. HA 和 HB 必须在同一子网内

B. HA 和 HB 必须在不同子网内

C. HA 和 HB 无论在一个子网或不在一个子网都可以

D. HA 和 HB 必须使用相同的操作系统

试题（12）分析

本题考查 LAN、VLAN 的概念、IP 子网与物理网络的映射关系以及 IP 选路原理。

LAN 是物理上的一个广播域，在 LAN 的所有设备都能收到其他设备的广播信息。

VLAN 是逻辑上的广播域，可以把一个 LAN 划分为多个 VLAN。划分 VLAN 后，LAN 内的设备以 VLAN 为单位组成广播域。

在 IPv4 网络中，一个 IP 子网只能映射一个 LAN 或 VLAN；多个 IPv4 子网，可以映射到一个 LAN 或 VLAN 中。

同一子网内主机可直接通信；不同子网之间，主机必须通过路由器才能进行通信。

参考答案

（12）A

试题（13）

假定一个 IPv4 网络由 4 段不同的 LAN 互联而成，每段 LAN 上的最大 MTU 值分别是 512、1024、2048 和 4096，则在这个 IPv4 网络上可能出现 IPv4 分组（IP Packet）的最大长度是（13）。

（13）A. 512　　B. 1024　　C. 2048　　D. 4096

试题（13）分析

本题考查 IPv4 网络中 MTU 的概念和应用。

IPv4 网络中，IPv4 分组（即数据包）的理论最大长度为 65535 字节（参考试题 11 分析中的 IPv4 数据包格式）。但实际应用时，IPv4 分组的长度受制于底层（二层协议）可传送的最大数据长度。MTU（最大传输单元）是指 IP 协议底层（二层）能够传输的最大数据单元长度，单位为字节。

每个 LAN 网段上的 IPv4 子网的底层（二层）网络技术可能是不同的，因此 MTU 的数值也不相同。在每个 LAN 网段上能够传输的最大 IPv4 分组（即数据包）等同于本 LAN 网段的 MTU。如果四个 LAN 网段能够彼此了解相互的 MTU 值，则最大 IPv4 分组长度为 MTU 值的最小值；如果四个 LAN 网段彼此由于某种原因而不能相互了解，则 IPv4 分组的最大长度有可能是最大的 MTU 值（每个 LAN 网段上的 IPv4 分组最大长度分别等于各 LAN 网段上的 MTU 值）。

IPv4 分组长度大于本 LAN 网段内的 MTU 值时，IPv4 分组将进行分段和重组。

参考答案

（13）D

试题（14）

一个稳定的 RIP 网络中的一个路由器需要通告 20 条路由，这些路由需要通过一个 UDP 报文来传送。如果这个 UDP 报文每 30 分钟丢失一次，那么对网络路由的影响是 (14) 。

（14）A. 对路由器有影响　　B. 对网络有影响

C. 对路由器和网络都没有影响　　D. 对路由器和网络都有影响

试题（14）分析

本题考查 RIP 协议的工作原理，重点考查广播周期和老化周期。

（1）RIP 协议

RIP 协议有两个版本：RIP1 和 RIP2。RIP 协议中使用 32 位的因特网地址。路由表中的每一项，可以表示一个主机、一个网络或一个子网。RIP 协议中，路由器需要自己分析路由信息中的地址是代表网络还是主机（参阅 IP 地址分类和子网掩码原理部分）。RIP 协议支持"默认路由"的路由选择方法，默认路由以"0.0.0.0"在路由表中来表示本区域以外的网络路径。

在缺省状态下，RIP 使用非常简单的度量制式（路由表中的开销）：距离是通往目的站点所需经过的链路数——即"跳数"，是取值在 1～15 之间的整数；数值 16 表示无穷大的距离（防止"计数到无穷大"现象）。

RIP 对点到点连接和广播型网络（如以太网）都提供支持。RIP 分组使用 UDP 协议传输。RIP 进程使用 UDP 端口 520 来进行发送和接收。在 RIP 网络中，分组以广播的形式进行发送，所有与之相连的路由器都会接收该分组。

RIP 分组的定时广播周期是 30s，每个 RIP 网络中的路由器都按该周期定时发送自己的路由表信息（距离向量广播）。RIP 中，路由信息的有效时间是有限制的，规定为 180s，如果 180s 时间内该路由信息未被刷新，则相应的距离被设定为无穷大，该路由记录会从路由表中删除。注意，由于 RIP 网络中，路由器每隔 30s 广播一次自己的路由表信息，因此路由器的路由记录会不断地被刷新（路由记录数据可能不会变化，但收到相同的路由信息即为刷新）。

（2）RIP1 和 RIP2

RIP1 是 RIP 的第一个版本，在广播 RIP 路由信息时，RIP 分组中只包含两个主要的数据项：目的（主机或网络）和到达目的的距离。RIP1 不能支持 AS，不能以子网选择路由。为了适应因特网的发展，开发了第二代 RIP 协议 RIP2。

RIP2 是 RIP1 的改进版，主要增加了以下功能：

- 支持以子网选择路由（支持子网掩码）。
- 支持与 AS 互通（支持 AS 间路由）。

- 支持验证机制和多点广播功能。

（3）结论

一个稳定的 RIP 网络即为网络拓扑结构不再变化，路由表稳定，此时 RIP 分组 30s 广播一次，路由老化周期为 180s。如果每 30 分钟丢失一次路由器广播 UDP 报文，则不会对路由器和网络产生任何影响。

参考答案

（14）C

试题（15）

在一个子网中有一个主机 HA 和路由器 RX，HB 是其他子网的主机。在主机 HA 中到 HB 的路由是 RX（HA 经 RX 到达 HB）。假定在 HA 和 RX 的子网中再增加一个路由器 RY，想让 HA 经 RY 到达 HB，此时需要（15）。

（15）A. RY 发送路由重定向 ICMP 报文给 HA
B. RX 发送路由重定向 ICMP 报文给 HA
C. RY 发送路由重定向 ICMP 报文给 HB
D. RX 发送路由重定向 ICMP 报文给 HB

试题（15）分析

本题重点考查 ICMP 协议中路由重定向的概念。

Internet 网络中的设备可分为路由器和主机两种，在路由器和主机中都需要具有正确的路由表网络才能正常的工作。

在 Internet 中，路由信息的传输分为两种：一种是路由器和主机之间的路由信息传递，它是由 ICMP 的路由功能完成的；另一种是路由器和路由器之间路由信息的交换，它们要依靠特殊的协议来完成，这些特殊的协议就是路由协议。无论 ICMP 协议还是路由协议，最终要在各自的结点上（包括主机和路由器）维护一个正确的路由表，以路由表决定如何发送（针对主机）和转发（针对路由器）IP 分组。

ICMP 的路由功能包括两个功能：一是发现本地路由器；二是路由重定向。 下图显示了 ICMP 报文的路由器广告报文格式（类型=9）。

<table>
<tr><td>类型 ＝9</td><td>代码 ＝空</td><td>校验和</td></tr>
<tr><td>地址总数</td><td>地址表项大小</td><td>有效时间</td></tr>
<tr><td colspan="3">路由器地址　〔1〕</td></tr>
<tr><td colspan="3">优先选择级别　〔1〕</td></tr>
<tr><td colspan="3">路由器地址　〔2〕</td></tr>
<tr><td colspan="3">优先选择级别　〔2〕</td></tr>
</table>

路由器广告报文包含路由器地址列表以及优先级选择级别。ICMP 报文给出了类型值为 9，代码字段为空，表中地址总数和每个表项的大小以及路由器声明的“有效时间”。

发布路由器广告通常目的地址为 224.0.0.1（ICMP 报文在 IP 报文中发送，使用 D 类的组播地址），该地址代表一个 IP 网络（路由器在哪个网络上广告就代表哪个网络）上的所有主机。如果网络不支持组播地址 224.0.0.1，则使用有限广播地址 255.255.255.255。路由器一般每隔 7min 广播一次路由器广告。路由器广告的有效时间一般是 30min。

如果主机刚开始工作时，得不到网络上的路由器地址，它可以发送路由器请求报文，其格式如下图所示。

类型 ＝10	代码 ＝空	校验和
保留		

路由器请求报文目的地址是 224.0.0.2，它代表一个 IP 网络上的所有路由器。收到该请求报文的路由器，可以直接给请求主机发送响应报文（实际上是路由器广告报文）或广播路由器广告报文。

主机收到具有多个路由器地址和优先级的路由器广告后，通过比较网络地址（由子网掩码确定），忽略不属于本网络的路由器地址。在属于本网络的路由器地址中，挑选优先级最高的路由器地址作为主机的默认路由器。当主机的 IP 分组到达本网络以外的 IP 网络时，如果没有明确的路径到达目的地，则主机的 IP 分组都通过默认路由器进行转发。

默认路由是网络运行的一种好的方法。但有时会增加新的路径。这时需要使用 ICMP 的路由重定向功能。路由重定向报文格式如下图所示：

类型 ＝5	代码＝0,1,2,3	校验和
因特网地址		
因特网包头 ＋64 数据		

路由重定向功能可以让本地主机从默认路由器得到到达目的地更好的路径。过程如下：

- 主机正常发送分组给默认路由器；
- 默认路由器发现有到达目的地更好的路径；
- 默认路由器发送路由重定向报文给主机，重定向报文中含有最佳路径的路由器地址；
- 主机在本机路由表中增加达到该目的地的新路径。

参考答案

（15）B

试题（16）

在 DNS 中，域名是倒树状结构。树根称之为“根域”，根域下面是“顶级域名”。顶级域名中有个“arpa”的顶级域名，其作用是（16）。

（16）A. ARPAnet 组织的简称，是 ARPA 组织的域名

B. Arpa 国家的简称，是 arpa 国家的域名

C. 用作反向地址解析

D. 一个普通的顶级域名

试题（16）分析

本题考查对 arpa 域名的理解。

DNS 一般是用来通过域名来解析 IP 地址的域名服务系统。DNS 也可以用来做反向解析，即通过 IP 地址得到域名。反向解析使用的域名为 in-addr.arpa。

参考答案

（16）C

试题（17）

建立 TCP 连接时需要三次握手，而关闭 TCP 连接一般需要 4 次握手。由于某种原因，TCP 可能会出现半关闭连接和半打开连接这两种情况，这两种情况的描述是（17）。

（17）A. 半关闭连接和半打开连接概念相同，是同一现象的两种说法

B. 半关闭连接是一端已经接收了一个 FIN，另一端正在等待数据或 FIN 的连接；半打开连接是一端崩溃而另一端还不知道的情况

C. 半打开连接是一端已经接收了一个 FIN，另一端正在等待数据或 FIN 的连接；半关闭连接是一端崩溃而另一端还不知道的情况

D. 半关闭连接是一端已经接收了一个 FIN，另一端正在等待数据或 FIN 的连接；半打开连接是一端已经发送了 SYN，另一端正在等待 ACK 的连接

试题（17）分析

本题考查对 TCP 连接的建立过程和 TCP 连接的关闭过程的理解。

（1）TCP 连接的建立

TCP 协议是面向连接的协议，提供可靠的、全双工的、面向字节流的、端到端的服务。TCP 连接是在无连接的 IP 协议上建立的。

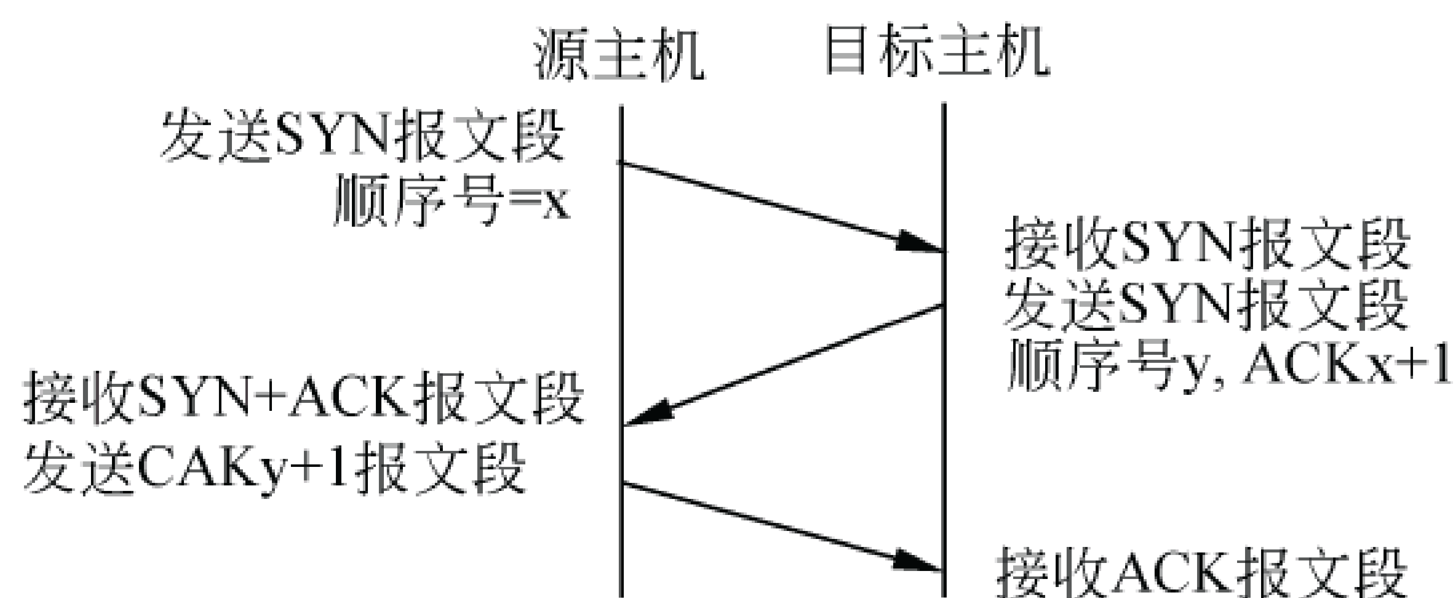
TCP 连接建立：TCP 的连接建立过程又称为 TCP 三次握手。首先发送方主机向接收方主机发起一个建立连接的同步（SYN）请求；接收方主机在收到这个请求后向发送方主机回复一个同步/确认（SYN/ACK）应答；发送方主机收到此包后再向接收方主机发送一个确认（ACK），此时 TCP 连接成功建立。

（2）TCP 建立连接过程

TCP 会话通过三次握手来初始化。三次握手的目标是使数据段的发送和接收同步。同时也向对方主机表明其一次可接收的数据量（窗口大小），并建立逻辑连接。这三次握手的过程可以简述如下：

- 源主机发送一个同步标志位（SYN）置 1 的 TCP 数据段。此段中同时标明初始序号（Initial Sequence Number，ISN）。ISN 是一个随时间变化的随机值。
- 目标主机发回确认数据段，此段中的同步标志位（SYN）同样被置 1，且确认标志位（ACK）也置 1，同时在确认序号字段表明目标主机期待收到源主机下一个数据段的序号（即表明前一个数据段已收到并且没有错误）。此外，此段中还包含目标主机的段初始序号。
- 源主机再回送一个数据段，同样带有递增的发送序号和确认序号。

至此为止，TCP 会话的三次握手完成。接下来，源主机和目标主机可以互相收发数据。整个过程如下图所示。



TCP 建立连接的三次握手过程

（3）TCP 释放连接过程

建立一个连接需要三次握手，而终止一个连接要经过四次握手。这由 TCP 的半关闭（half-close）造成的。既然一个 TCP 连接是全双工（即数据在两个方向上能同时传递），因此每个方向必须单独地进行关闭。

TCP 连接的释放需要进行四次握手，步骤是：

- 源主机发送一个释放连接标志位（FIN）为 1 的数据段发出结束会话请求。
- 目的主机收到一个 FIN，它必须通知应用层对端已经终止了那个方向的数据传送，同时向源主机发回一个确认，并将应答信号（ACK）设置为收到序号加 1，这样就终止了这个方向的传输。
- 目的主机此时依然可以向源主机发送数据，数据发送结束后，目的主机也发出一个 FIN 置 1 的报文，请求终止本方向的连接。
- 源主机收到 FIN，再回送一个数据段，带有递增的确认序号。

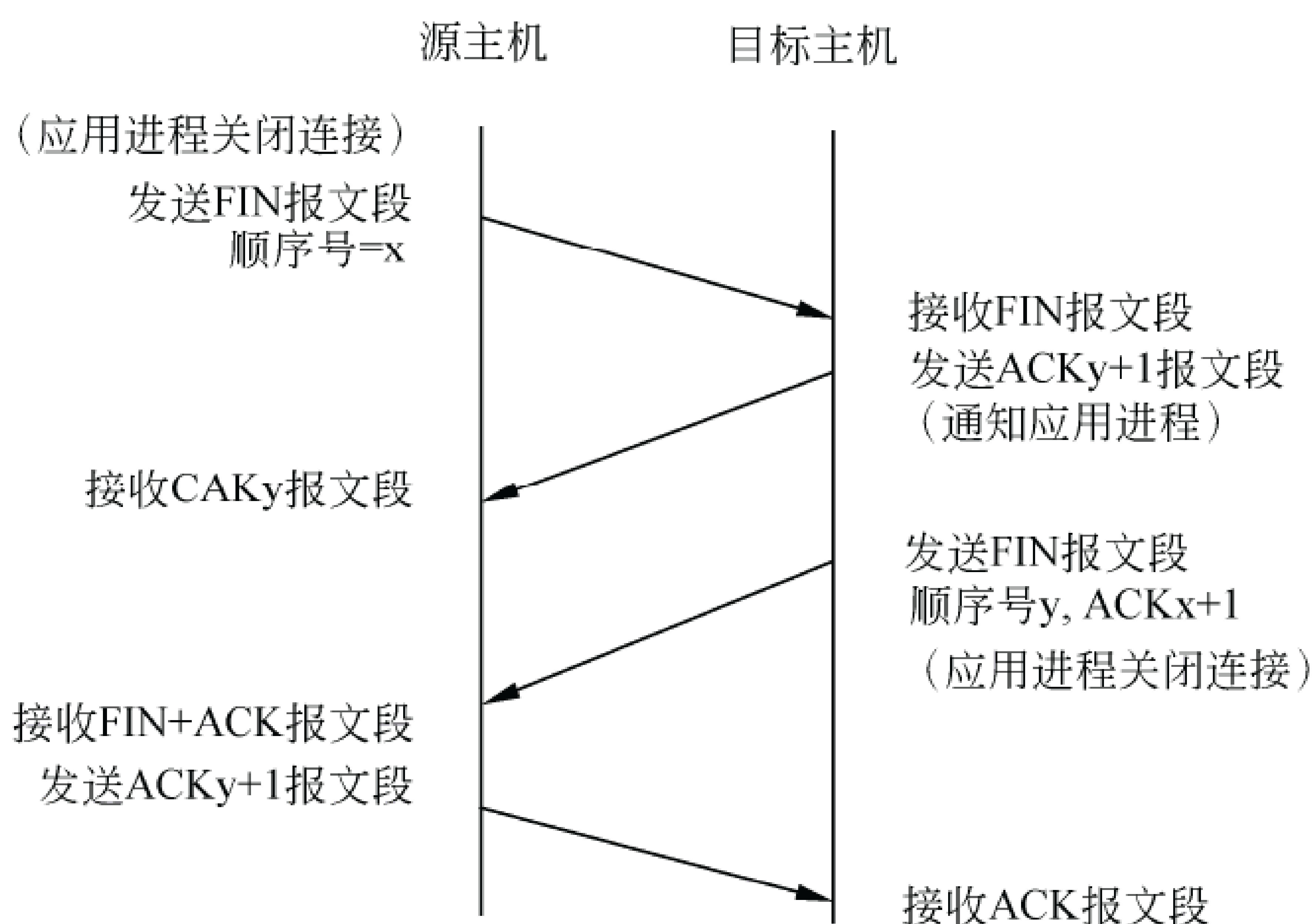
TCP 释放连接的四次握手过程

（4）半打开连接和半关闭连接的概念

TCP 连接经三次握手建立后，如果一方已经关闭或异常终止连接而另一方却还不知

道，我们称这样的 TCP 连接为半打开（half-open）连接。任何一端的主机异常都可能导致发生这种情况。只要不打算在半打开连接上传输数据，仍处于连接状态的一方就不会检测另一方已经出现异常。TCP 的 Keepalive 定时器用于发现并结束半打开连接。

TCP 连接建立后，TCP 提供了双向的数据通路。TCP 提供了其中一端结束它的发送后还能接收来自另一端数据的能力，这称为半关闭。半关闭是 TCP 连接关闭过程中完成了前半部分的状态，这时只关闭了一个方向上的数据通道，另一个方向上仍然能够继续数据传输。



参考答案

（17）B

试题（18）

IPv6 与 IPv4 相比，下列叙述正确的是<u>（18）</u>。

（18）A. IPv6 地址也分为 A、B、C、D、E 五类

B. IPv6 网络可直接使用 IPv4 的路由协议

C. IPv6 不能实现地址自动配置

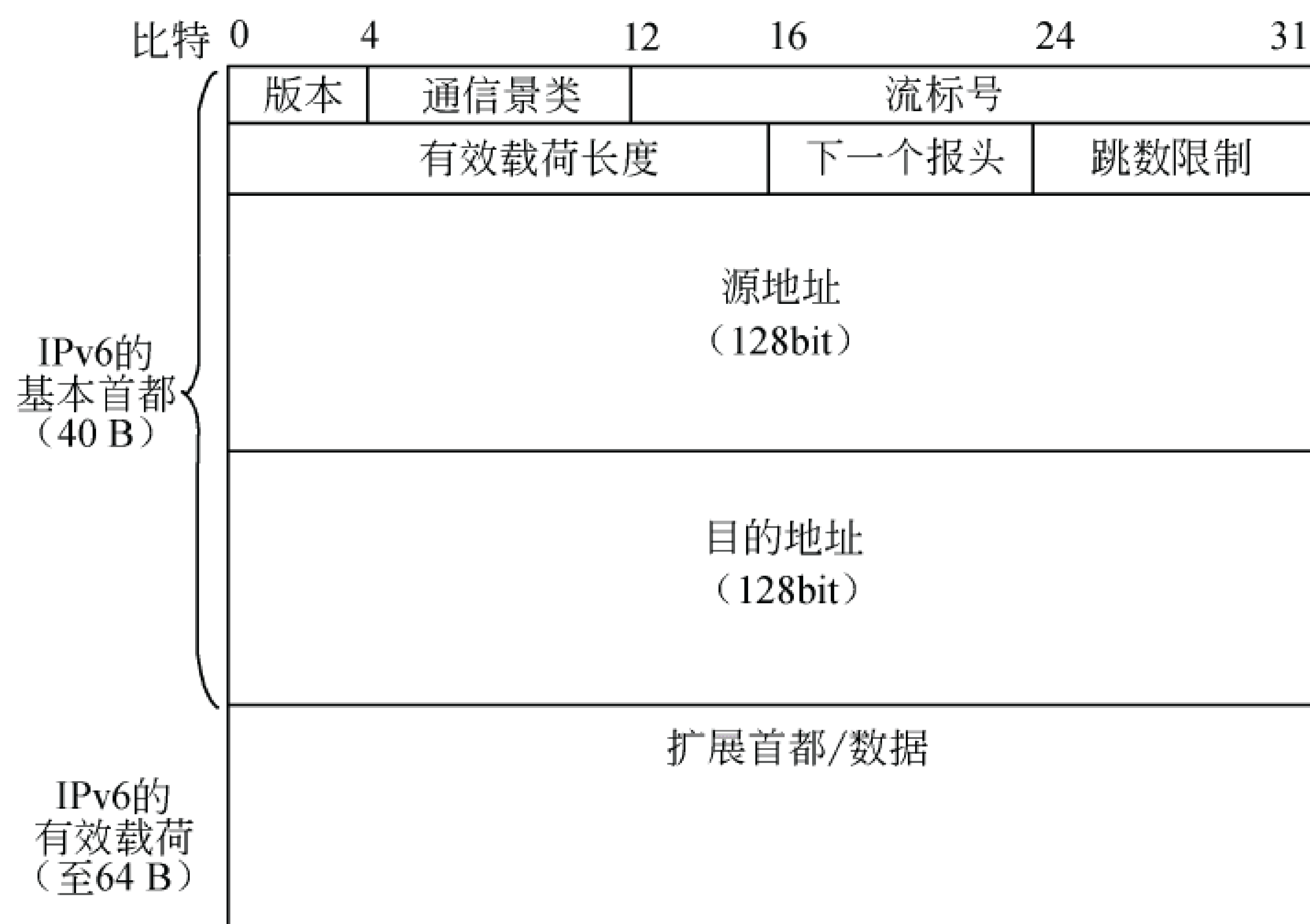
D. IPv6 分组的头中增加了流标签（Flow Label）字段

试题（18）分析

本题考查对 IPv6（与 IPv4 相比）变化的理解。

IPv6 地址分类与 IPv4 不同，不再分为 A、B、C、D、E 五类；IPv6 中的路由协议不能直接使用 IPv4 的路由协议；IPv6 中可以实现链路本地地址的自动配置；IPv6 的分组头中增加了流标签字段。

IPv6 分组（即数据包）格式如下图所示：



图中的流标号即流标签字段，英文原文为 Flow Label。

参考答案

（18）D

试题（19）

一个单位内部的 LAN 中包含了对外提供服务的服务器（Web 服务器、邮件服务器、FTP 服务器）、对内服务的数据库服务器、特殊服务器（不访问外网）以及内部个人电脑。其 NAT 原则是：<u>（19）</u>。

（19）A. 对外服务器作静态 NAT；个人电脑作动态 NAT 或 PAT；内部服务器不作 NAT

B. 所有的设备都作动态 NAT 或 PAT

C. 所有设备都作静态 NAT

D. 对外服务器作静态 NAT；内部服务器作动态 NAT；个人电脑作 PAT

试题（19）分析

本题考查 NAT 的概念；静态 NAT 和动态 NAT 的应用原则。

IPv4 地址资源有限，面临无地址分配的问题。如何解决呢？方法主要有两个：

方法一：当然是高效利用 IP 地址资源。如减少浪费，把大网如一个 A 类网络，分为子网来进行分配。子网的应用现在已经非常普遍。

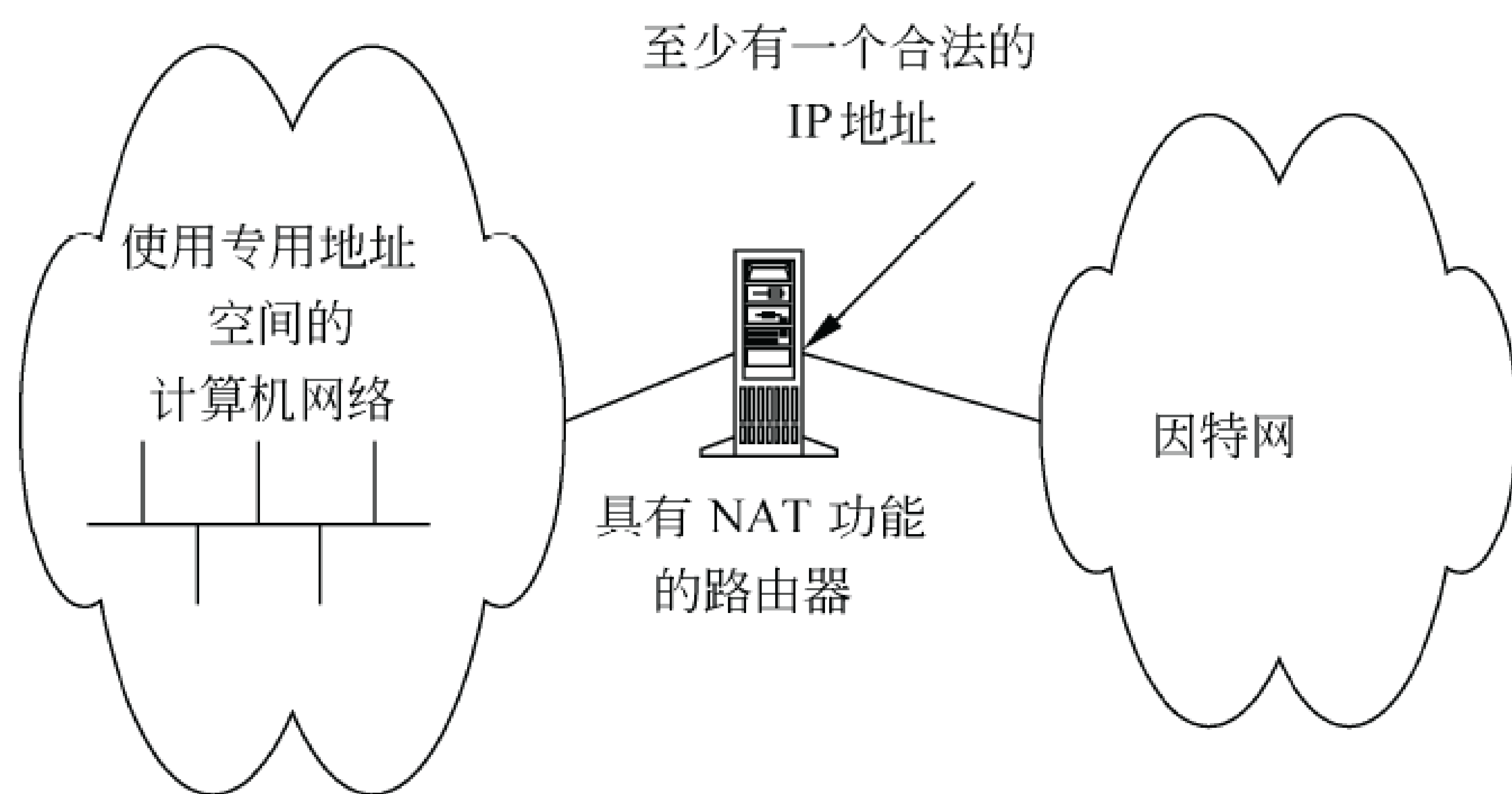
方法二：在 Internet 中定义了专用地址空间（RFC1918）如下：

- 1 个 A 类地址： 10.0.0.0～10.255.255.255
- 16 个 B 类地址： 172.16.0.0～172.31.255.255
- 256 个 C 类地址： 192.168.0.0～192.168.255.255

这些地址称为私用地址或专用地址，用户不需要向任何人申请，就可以直接使用；

但是这些地址不允许出现在公共的 Internet 上。那么用户要访问公共的 Internet 怎么办呢？这要用到地址翻译 NAT（Network Address Translate）技术。

NAT 应用的典型场景如下所示。



这里完成 NAT 功能的路由器或其他设备必须有一个合法的公共 Internet 地址（简称公网 IP 地址）。当私网用户需要访问公网时，通过（私网 IP 地址，端口号）与（公网 IP 地址，端口号）的转换进行访问。

目前的地址转换方式主要有三种，分别是 NAT、PAT 和 Proxy。

NAT：提供一个公网的 IP 地址池，私网用户需要访问公网时，进行公网 IP 地址和私网 IP 地址的映射。

PAT：只提供一个公网的 IP 地址，私网用户需访问公网时，多个私网地址对应一个公网 IP 地址，通过附加端口号来识别。

Proxy：工作在应用层，由代理软件完成数据包的地址转换。

目前，NAT 一词可以代表 NAT 和 PAT 的统称，即包含一对一映射和多对一映射。NAT 在实现时又可分为静态 NAT 和动态 NAT。

静态 NAT：一个（私网 IP 地址，端口号）对应一个（公网 IP 地址，端口号），映射关系由人工指定保持静态不变。主要应用于专网或内部网络上对外提供服务的设备。

动态 NAT：一个（私网 IP 地址，端口号）对应一个（公网 IP 地址，端口号），但映射关系是动态的，由 NAT 设备根据运行情况随机确定。主要应用于专网或内部网络上的普通用户访问公网时的场景。

参考答案

（19）A

试题（20）

下面对电子邮件业务描述正确的是__（20）__。

（20）A. 所有使用电子邮件的设备接收和发送都使用 SMTP 协议

B. 必须将电子邮件下载到本地计算机才能查看、修改、删除等

C. 必须使用专用的电子邮件客户端（例如 OutLook）来访问邮件

D. 电子邮件体系结构中包含用户代理、邮件服务器、消息传输代理和邮件协议

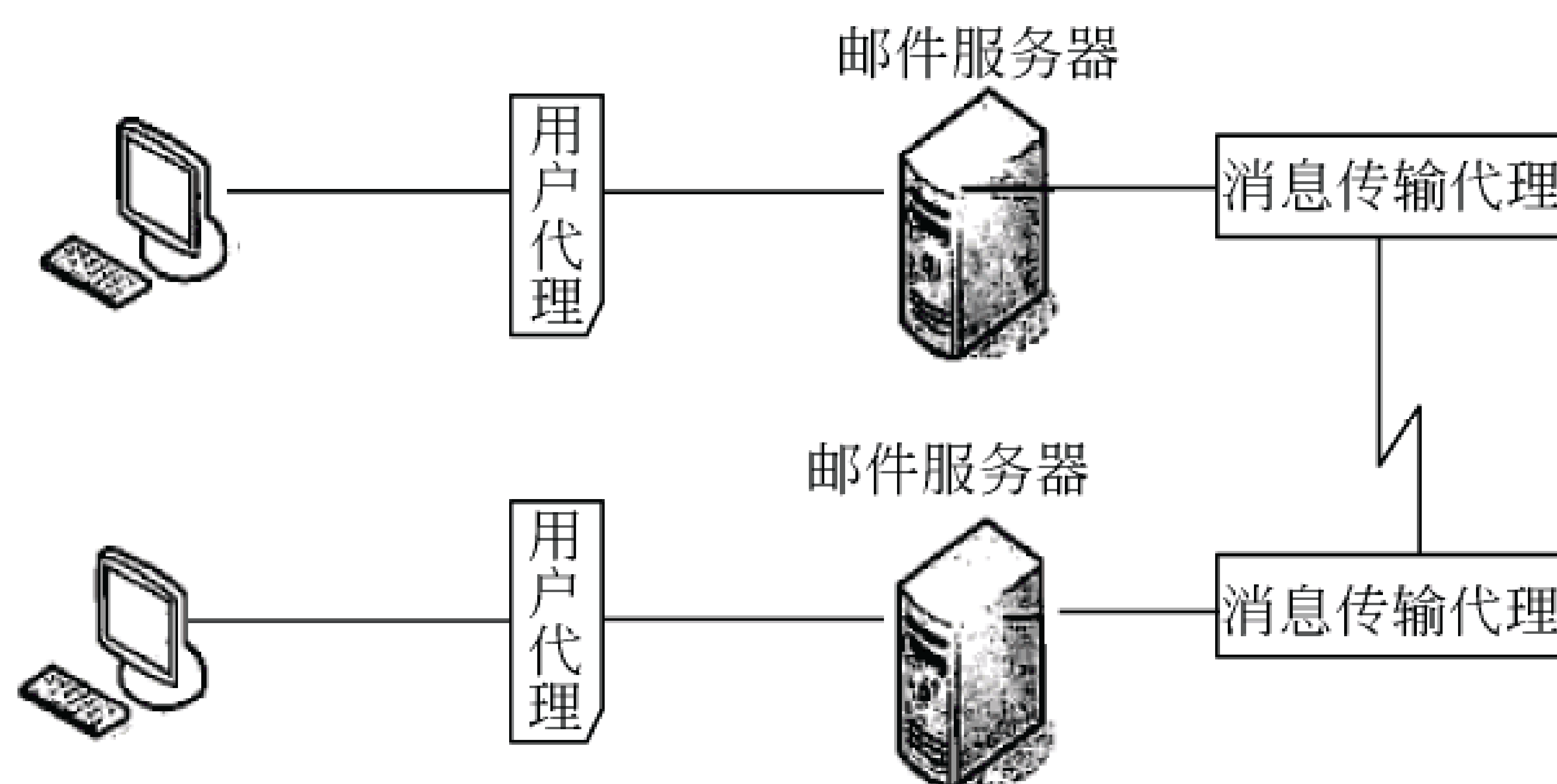
试题（20）分析

本题主要考查电子邮件（E-mail）系统的组成和所使用的协议。

（1）电子邮件体系结构

电子邮件服务是因特网基本的服务之一，是一种因特网上使用最广泛的服务。它提供一种快速、简便的信息传输手段。电子邮件系统是以电子信息传输手段传输以电子信息形式存储的邮件的系统。所谓电子邮件，就是以电子信息形式存储的信件。我们发送、接收邮件时是以电子手段进行处理的。

一个电子邮件体系结构中包含用户代理、邮件服务器、消息传输代理和邮件协议。如下图所示。



（2）POP3、SMTP 协议及服务器

一般邮件客户与邮件服务器之间需要某种协议以存取用户在邮件服务器上的邮件或发送邮件到邮件服务器。在这两个方向上，邮件客户和邮件服务器之间使用的协议是不同的。

SMTP 英文是 Simple Mail Transfer Protocol，意为简单邮件传输协议。是计算机之间传输电子邮件的协议。该协议主要规定基础的电子邮件提交系统怎么传递报文，即电子邮件怎么通过两个计算机之间的物理链路，从一个计算机传输到另一个计算机。SMTP 非常简单，它没有规定电子邮件系统怎样从用户接收邮件等。用户从邮件服务器上接收邮件要使用 POP3 协议。

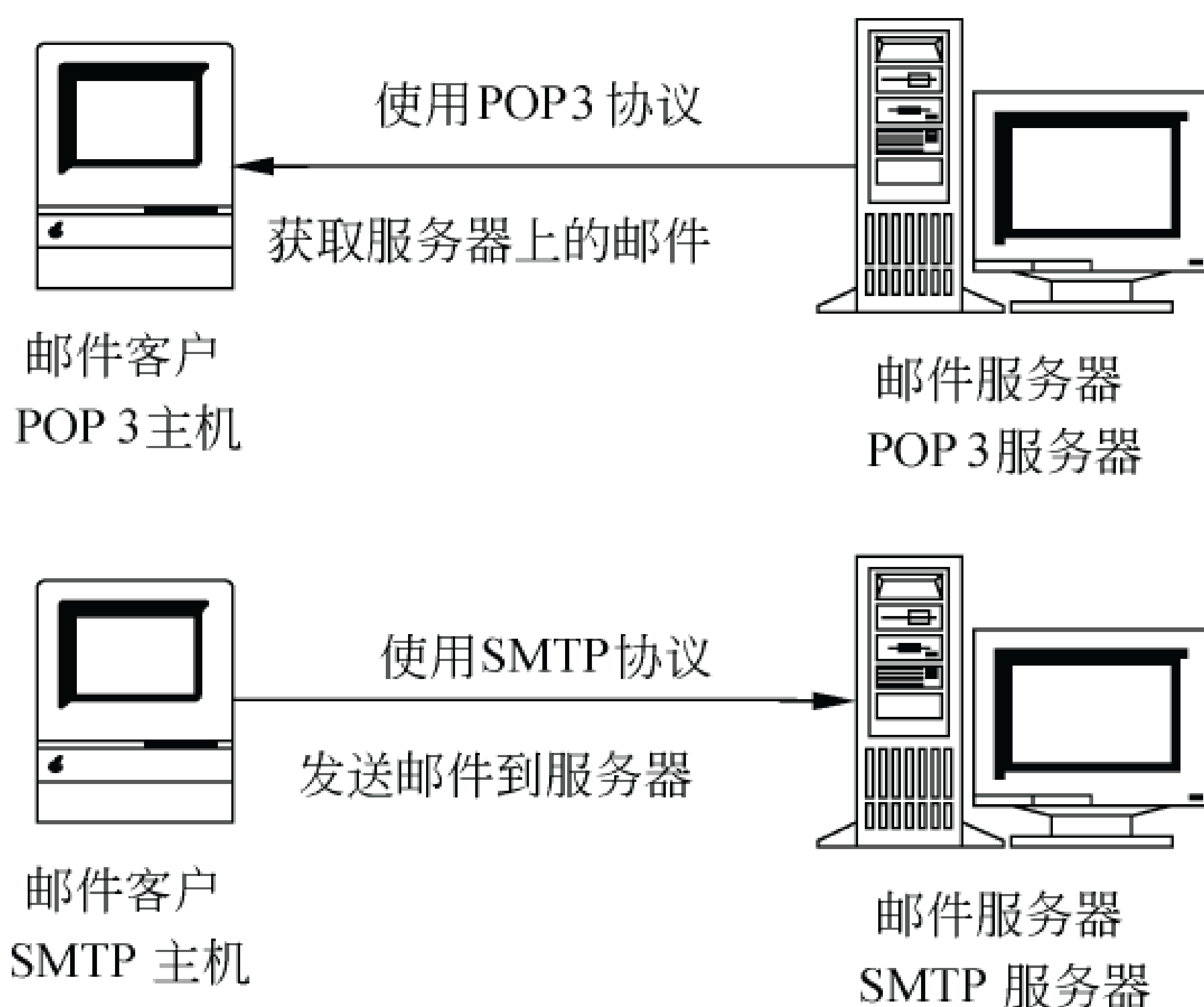
POP 英文是 Post Office Protocol，意为邮局协议，POP3 是这个协议的版本 3。它使邮件客户可以用一种比较实用的方法来访问存储于服务器上的邮件。通常，这意味着邮件客户可以从服务器上取得邮件，而服务器为它暂时保存邮件。

下页图中表明了这两种服务器的作用。邮件客户在发送和接收时，使用的是不同功能的服务器。这两个服务器可以由一个计算机完成，也可以是两个不同的计算机。

（3）IMAP4 协议

IMAP rev1（RFC2060）是 Internet Message Access Protocol 的缩写，是通过 Internet

获取信息的一种协议。IMAP4 是 IMAP 协议的第 4 个版本，正如 POP3 是 POP 协议的第 3 个版本一样。IMAP 是一种强有力的邮箱访问方式。



POP3 提供了快捷的邮件下载服务，用户可以利用 POP3 把邮箱里的信下载到 PC 上进行离线阅读。一旦邮件进入 PC 的本地硬盘，就可以选择把邮件从服务器上删除，然后脱离与 Internet 的连接并选择在任何时候阅读已经下载的邮件。

IMAP 支持用户在线阅读功能，支持 WebMail 功能（不下载到本地，所有邮件都在邮件服务器上），允许用户在服务器上建立任意层次结构的文件夹，并且可以灵活地在文件夹之间移动邮件，随心所欲地组织你的邮箱。当然，IMAP 也支持邮件下载到本地阅读（等同 POP3 功能）。

参考答案

（20）D

试题（21）

在互联网上，当我们访问一个设备时，<u>（21）</u>。

（21）A. 必须要有域名，才能访问

B. 有 IP 地址就可以访问

C. 必须同时有 IP 地址和域名

D. 必须要有域名服务器

试题（21）分析

本题主要考查对 IP 地址和域名作用的理解。

在 Internet 上通信，需要 IP 地址即可进行。域名系统是为了便于人们记忆需要的互联网（Internet）服务而产生的。

比如，通过浏览器访问新浪网www.sina.com.cn，系统首先通过 DNS 系统查找到该域名对应的 IP 地址（正向解析），然后把用户信息封装为 IP 分组（数据包）进行传输和

通信。

参考答案

（21）B

试题（22）

对于一个稳定的 OSPF 网络（单区域），下面描述正确的是__（22）__。

（22）A. 必需指定路由器的 Router ID，所有路由器的链路状态数据库都相同

B. 无需指定路由器的 Router ID，路由器之间的链路状态数据库可以不同

C. 定时 40s 发送 Hello 分组，区域中所有路由器的链路状态数据库都相同

D. 定时 40s 发送 Hello 分组，区域中路由器的链路状态数据库可以不同

试题（22）分析

本题考查对单区域 OSPF 工作原理的理解。

（1）OSPF 概念

OSPF 即开放最短路径优先协议（Open Shortest Path First），是为了解决距离矢量类路由选择协议存在的问题而开发的。

RIP 协议是最早出现的路由协议，它采用距离矢量路由算法进行路由信息传递，这种协议的中心思想是：定时更新路由表，选择开销最小的路由。距离矢量类选择协议的缺点是收敛速度慢、跳数限制以及容易产生环路等。

OSPF 协议属于链路状态路由选择协议，采用 SPF 算法来计算路由表。OSPF 协议的核心思想是：网络中的每个路由器都有一个相同的唯一的网络图（链路状态数据库），通过 SPF 算法，每个路由器独立计算出自己的路由表。这里每个路由器有两张表：“网络图”即链路状态数据库（LSDB）和路由表。OSPF 协议的主要功能是维护“网络图”的一致性和正确性，如果网络发生了变化，把变化传递给每个路由器，保证新的“网络图”反映最新的网络拓扑结构；同时每个独立的路由器根据最新的“网络图”，通过 SPF 算法，得到新的路由表。

（2）关键术语

- 链路：所谓链路就是在网络中两个路由器间的物理的或逻辑的连接，链路状态包括传输速度、延迟、接口类型等一些属性。
- 网络图：即链路状态数据库（LSDB）。OSPF 网络中，所有连接路由器的逻辑的或物理的链路信息的总和。实际上就是网络的拓扑结构组成图。
- 路由器标识符（RouterID）：用于标识每个路由器的 32 位数。通常，一个路由器有多个接口（Interface），包括物理接口和虚拟接口（loopback），每个接口都会分配 IP 地址，那么如何标识这个路由器呢？原则是：使用所有接口中 IP 地址最大 IP 数值来标识该路由器，称为 RouterID。如果在路由器上使用了 loopback 接口，优先选择 loopback 的最高 IP 地址。

（3）Hello 协议和扩散协议

OSPF 由两个互相关联的主要部分组成：Hello 协议和扩散（Reliable Flooding）机制。Hello 协议用于检测邻居是否可达；Hello 协议操作在每个活跃的 OSPF 接口上，它使用的组播地址使得这些流量不会对非 OSPF 的路由器造成影响。扩散算法确保 OSPF 区域中所有路由器具有完全一致的链接状态数据库。

OSPF 协议支持在广播型网络（如以太网）、点到点网络和非广播型网络（NBMA 网络，如 FR、ATM 等）上的运行。其 Hello 协议的参数选择如下：

OSPF 环境	Hello 间隔	Down 机判定间隔
广播	10 秒	40 秒
点对点	10 秒	40 秒
NBMA	30 秒	120 秒

以广播型网络（以太网）为例，每 10 秒发送一个 Hello 包，如果 40 秒内收不到邻居发送的 Hello 包，则判断邻居不可达。

（4）结论

一个稳定的 OSPF 单区域网络，网络的拓扑结构稳定，即 LSDB 中的链路不发生变化，此时所有的路由器中的 LSDB 都相同。

参考答案

（22）A

试题（23）

下列对 FTP 业务的描述正确的是<u>（23）</u>。

（23）A. FTP 服务必须通过用户名和口令才能访问。FTP 可以基于 UDP 或 TCP 传输信息

B. FTP 服务器必须通过用户名和口令才能访问。FTP 只能基于 TCP 传输信息

C. FTP 服务器无须用户名和口令即可访问。FTP 可以基于 UDP 或 TCP 传输信息

D. FTP 服务器无须用户名和口令即可访问。FTP 只能基于 UDP 传输信息

试题（23）分析

本题考查对数据业务的理解和对 FTP 业务的访问机制的理解。

FTP 业务属于文件传输类的数据业务。针对 Internet 网络而言，文件传输要保证可靠性（文件传输不能有差错），对实时性要求不高（可以有大的延迟或延迟抖动）。因此 FTP 业务是基于 TCP 协议而实现的。

FTP 在用户下载时需要提供用户名的口令；即使是匿名登录，其实本质上也是有用户名（anonymous）和口令（任意邮箱格式 xxx@xx.xxx）。

参考答案

（23）B

试题（24）

下列对集成服务（IntServ）模型和区分服务（DiffServ）模型描述正确的是（24）。

（24）A. IP 的 QoS 技术主要是集成服务模型和区分服务模型

B. 集成服务模型和区分服务模型无法进行结合

C. 集成服务扩展性好，可以应用在不同规模的网络中；区分服务扩展性差，不能应用在大型网络中

D. 集成服务模型可以针对单个业务（比如一路电话）进行 QoS 保证；区分服务模型不针对单个业务，而是针对一类业务进行 QoS 保证

试题（24）分析

本题主要考查对集成服务（IntServ）模型和区分服务（DiffServ）模型的理解。

（1）IP QoS 技术

在通信和计算机网络中，服务质量简称 QoS。QoS 分广义和狭义之分：狭义的 QoS 指技术指标（传输时延、抖动、丢失率、带宽要求、吞吐量等）；广义的 QoS 指资源调配与利用、层与层之间的协商，从而涉及不同层次的 QoS。

QoS 在 IETF 中的定义为“A set of service requirements to be met by the network while transporting a flow”，即网络在传输数据流时要满足的一系列服务要求，具体可量化为狭义的 QoS 技术指标。

Internet 最初是面向非实时的、数据类型通信而设计的。IP 协议提供无连接的、不可靠的、尽力而为的网络层服务。传统的 IP 传输服务被称为尽力而为的服务（Best Effort Service）。

尽力而为类型的服务无法满足对实时性要求较高的业务（如电话、视频业务等）的要求，于是 IETF 提出借鉴 QoS 技术，加强实现资源的控制和调度机制，使得网络能够支持各种类型的业务；为此 IETF 提出了综合服务模型（Interagted Service architecture，简称 IntServ，中文也翻译为综合服务体系）和分类业务模型（Differentiated Service Achitecture，简称 DiffServ，中文也翻译为区分服务体系）。

（2）集成服务（IntServ）模型

IntServ 是根据每个 IP 流 QoS 等级的精确描述，由具有 RSVP 功能的路由器中的 RSVP 协议和流的接纳控制支持 IP 的 QoS 分类。集成服务模型可以针对单个业务（由流来标识）进行端到端的 QoS 保证服务。

在 IntServ 流中，定义了三类业务——保证业务（Guaranteed Service，GS）、受控负载业务（Controlled Load Service，CLS）和尽力而为的服务（Best Effort Service，BES）。对于 GS 业务，流的最大排队时延是受到控制的，路由上的任何时延都会影响最大排队时延。而 CLS 没有固定的时延保证，但业务流要与在网络轻载情况下的流质量相当，实

际上 CLS 要求有长期的带宽保证。总之，这两种业务都要求用令牌漏斗协议来定义流的特性，超出的业务流被当作 BES 型业务量处理。BES 业务是传统的 IP 服务提供的业务类型。

IntServ 中定义 RSVP 为其 QoS 信令。通过 RSVP，用户可以给每个业务流申请资源预留，要预留的资源可以包括缓冲区及带宽大小。这种预留需要在路径上的每一跳上进行，这样才能提供端到端的 QoS 保证。

利用资源预留可以使路由器能够提前决定是否有能力满足业务的需求，为每个流预留需要的网络资源，并建立相应的策略控制信息，即所谓“软状态”。

“软状态”信息在路由器上等同增加了转发策略，即附加的路由转发策略。这样路由器需要维护的“软状态”信息的数量与业务流的数量是线性关系。因此 IntServ 在具体实现时，其主要缺点就是扩展性较差，在骨干网上，业务流的数量十分庞大，路由器无法完成相应量级的“软状态”处理和资源预留工作。

（3）分类业务（DiffServ）模型

IETF 的 DiffServ 模型是基于每跳行为（Per Hop Bahaviors，PHB）的概念，DiffServPHB 由路由上的每个本地路由器所具有的前转行为来定义。目前，IETF 已定义两种主要的 PHB：

- 加速前转 PHB（Expedited Forwarding PHB，EF-PHB）

EF-PHB 的特征是带宽具有可配置性并在同一链路上不受其他业务量的影响。EF-PHB 可以用来在 DiffServ 域中建立要求具有低丢失率、低时延与低时延抖动的端到端业务。

- 可确定的前转 PHB 组（Assured Forwarding PHB Group，AF-PHB 组）

AF-PHB 组的特征是有 4 个 AF 等级，每个等级分配有一定量的转发资源（比如在一个 DiffServ 结点上的缓存与带宽等）。在每一个 AF 等级中，各个 IP 分组被标记上三种可能的丢弃优先级。当发生拥塞时，分组的丢弃优先级将决定在某一 AF 等级中各分组的相对重要性。4 个 AF 等级的相对性能之间没有标准的关系，AF-PHB 组可以实现以较高的可能性保证业务所要求的信息速率。

分类业务模型的核心思想是对业务流进行分类，针对不同种类的业务进行转发。在一个分类域中，所有的路由器都采用同样的转发策略——最终体系在 PHB；在一个分类域的边界进行业务流的分类和标记工作。

分类业余模型可以在 Internet 骨干网上大规模实现，但其不能针对单个业务流进行端到端的 QoS 保证。

（4）综合业务模型和分类业务模型的结合

这两种技术可以统合起来形成支持 QoS 敏感（aware）型 IP 业务的网络模型。在 IETF 给出的框架中，端到端的 QoS 是由网络边缘的 IntServ 区域与网络核心的 DiffServ 区域一起提供的，这一方式常被称为“核心边缘”方式。

参考答案

（24）D

试题（25）

MPLS 是一种将__（25）__路由结合起来的集成宽带网络技术。

（25）A. 第一层转发和第二层　　B. 第二层转发和第三层

C. 第三层转发和第四层　　D. 第四层转发和第七层

试题（25）分析

本题考查对 MPLS 技术核心思想的理解。

MPLS 最初是基于 ATM 技术发展起来的。它结合 ATM 技术和 IP 技术各自的优点。其核心思想是：边缘路由，核心交换。从协议层次上来观察即为：结合了第二层转发和第三层路由的集成宽带网络技术。

参考答案

（25）B

试题（26）

在一个局域网上，进行 IPv4 动态地址自动配置的协议是 DHCP 协议。DHCP 协议可以动态配置的信息是__（26）__。

（26）A. 路由信息

B. IP 地址、DHCP 服务器地址、邮件服务器地址

C. IP 地址、子网掩码、域名

D. IP 地址、子网掩码、网关地址（本地路由器地址）、DNS 服务器地址

试题（26）分析

本题考查 DHCP 协议的作用。

DHCP 中文翻译为动态主机配置协议，主要为要上网的设备动态配置上网参数。如果一个设备需要访问互联网，其必备的参数是：IP 地址、子网掩码、网关地址（本地路由器地址）；如果需要用域名访问互联网，则还需要配置 DNS 服务器地址。

参考答案

（26）D

试题（27）

BGP 是 AS 之间进行路由信息传播的协议。在通过 BGP 传播路由信息之前，先要建立 BGP 连接，称之为“BGP Session”。下列对 BGP Session 连接描述正确的是__（27）__。

（27）A. BGP Session 基于 IP 协议建立

B. BGP Session 基于 UDP 协议建立

C. BGP Session 基于 TCP 协议建立

D. BGP Session 基于 ICMP 协议建立

试题（27）分析

本题考查对 BGP 协议的了解。

边界网关协议（BGP）经历了不同的阶段，从 1989 年的最早版本 BGP1，发展到 1993 年开始开发的最新版本 BGP4。BGP4 支持 CIDR 和超网。

BGP 使用路径矢量路由算法，为了避免 AS 间的路由环路（距离矢量算法的缺点），AS 采用了路径向量的概念。路径向量是指，在传递到达某目的地（以 CIDR 形式的网络 ID 标识）的路由时，附加此路由经过的 AS 号。这样，当一个 AS 中的边界路由器收到某个路由时，只需要看看路径中是否包含有自己所在 AS 的号码便可判断是否有 AS 间环路。

BGP 是用来在自治系统（AS）之间传递选路信息的路径向量协议。BGP 利用了传输控制协议（Transmission Control Protocol，TCP）提供的可靠传输服务。这消除了 BGP 实现更新数据包的分段、重传、确认和先后顺序问题的需要，因为 TCP 已经完成了这些功能。另外，任何 TCP 使用的认证方法也可以利用于 BGP。

BGP 会话建立成功后，BGP 就使用通常的 Keepalive 消息来维护会话的完整性。Update 消息也可以重置保持计时器（hold timer），这一计时器的典型值是 keepalive 计时器（keepalive timer）值的 3 倍。如果连续 3 次收不到 Keepalive 消息，也没有 Update 消息，那么 BGP 会话就会被关闭。

参考答案

（27）C

试题（28）

P2P 业务和 C/S（或 B/S）结构的业务主要差别是<u>（28）</u>。

（28）A. P2P 业务模型中每个结点的功能都是等价的，结点既是客户机也是服务器
B. P2P 业务模型中的超级结点既是客户机也是服务器，普通结点只作为客户机使用
C. P2P 业务模型与 CS 或 BS 业务模型的主要区别是服务器的能力有差别
D. P2P 业务模型与 CS 和 BS 业务模型的主要区别是客户机的能力有差别

试题（28）分析

本题主要考查对 P2P 概念的理解。

C/S 是英文Client/Server的缩写，中文翻译为客户/服务器模式。C/S 结构的业务中 Client 和 Server 的功能和作用是不同的。Client 端主要完成业务的请求并处理和呈现返回结果；Server 端主要完成接收 Client 端提出的服务请求、进行相应的处理并将结果返回给 Client 端的功能。

C/S业务体系结构一般需要开发专用的客户端和服务器端软件，并针对不同的计算机操作系统开发不同的版本。其扩展性、服务升级的方便性、移植性都受到很大限制。

B/S 业务结构是基于 C/S 结构的，它们之间并没有本质的区别。B/S 是基于特定通

信协议（HTTP）的 C/S 架构，也就是说 B/S 包含在 C/S 中，是特殊的 C/S 架构。B/S 业务结构中客户端使用通用浏览器软件，Server 端使用基于通用的 Web 服务器的综合服务软件系统。

P2P 是英文 peer-to-peer 的简称，中文翻译为“对等网络”。P2P 是一种网络结构的思想，与目前网络中占据主导地位的C/S结构（包括 B/S）的一个本质区别是：整个网络结构中不存在中心结点（或中心服务器）。在 P2P 结构中，每一个结点（peer）大都同时具有信息消费者、信息提供者和信息通讯等三方面的功能。

在 P2P 网络中每一个结点所拥有的权利和义务都是对等的。从功能上说，每个结点（peer）既是客户机又是服务器，既能请求服务，也向其他结点（peer）提供服务。通俗地讲，P2P 可以直接将人们联系起来，让人们通过互联网直接交互。P2P 改变了互联网现在的以服务器为中心的状态、重返“非中心化”，并把权力交还给用户。

参考答案

（28）A

试题（29）

用 UTP cat5 作为通信介质，用一层以太网设备互联，最大联网距离是<u>（29）</u>。

（29）A. 100m　　B. 205m　　C. 500m　　D. 2500m

试题（29）分析

本题主要考查共享式以太网的联网法则。

（1）以太网组网和一层组网设备

组建以太网时如果不使用任何网络互连设备，其网络范围是有限的（受限于通信介质）。要扩大以太网的组网范围，可以使用互连设备完成。用于互连以太网的设备可以分为两类：第一层互连设备，称为中继器；第二层互连设备，称为网桥。

中继器从原理上看，是工作在 OSI 协议模型第一层的设备，即工作在物理层。它只对经过它的以太网信号进行放大。中继器的主要作用是把经过该设备的以太网信号进行整形、放大等处理后，以广播方式传送到设备的所有端口，目的是扩大以太网的物理覆盖范围，即连网的范围。

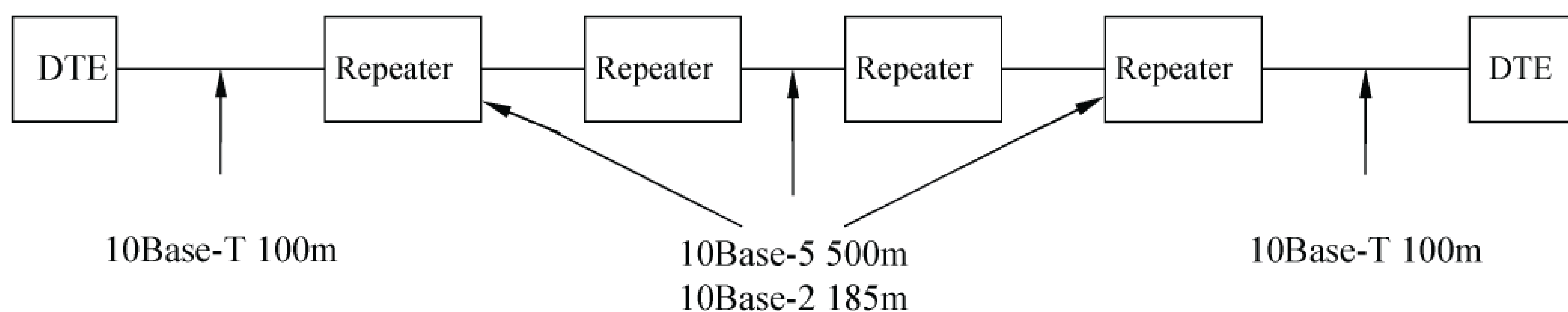
由于中继器设备只是简单的信号放大设备，用中继器互连的以太网，称为一个冲突域。中继器不能隔离以太网中的冲突（它对任何信号均放大广播，包括冲突信号）。

用中继器设备组网，又可称为共享式以太网组网。

（2）共享式 10Mbps 以太网组网原则

10Mbps 以太网有三个标准：10Base5、10Base2 和 10Base-T。共享式 10Mpbs 以太网组网原则是：5-4-3-2-1 法则，如下图所示。

5 是指用中继器互连的以太网中，两个结点（图中的 DTE 设备）之间最大可以有 5 个网段；4 是指最大可以有 4 个中继器；3 是有三个网段可以接入 DTE 设备（即计算机结点）；2 是有两个网段作互连网段；1 是指整个连网属于一个冲突域。



（3）10Base-T 共享式集线器组网

10Base-T 以太网中 T 表示传输介质是双绞线，所以 10Base-T 又称双绞线以太网。

双绞线有两种类型：非屏蔽双绞线 UTP 和屏蔽双绞线 STP。STP 双绞线外围有一层金属网称为屏蔽层，可以屏蔽外界电磁波辐射，抗干扰能力强，传输性能好，但价格高；UTP 由于没有屏蔽层，性能较差，但价格低廉。

目前双绞线以太网连网时一般使用 UTP，UTP 双绞线按其传输性能又分为几种：cat3、cat4、cat5、cat6 或更高，称为 3 类 UTP、4 类 UTP、5 类 UTP，数值越大，表明传输性能越好。UTPcat5，称为 5 类 UTP 双绞线，可以用于 10Mbps、100Mbps、1000Mbps 的以太网组网使用，是目前综合布线应用最广泛的通信介质。

在以上所述任何类型的双绞线中，一根双绞线内部包含 8 根绞合成 4 对的子线。简单讲就是，一根双绞线中有 4 对线。

10Base-T 连网介质使用 3 类或 5 类 UTP 或 STP；连网采用主机—集线器（HUB）模式，双绞线以太网中，共享式集线器就是中继器，应该遵守中继器的连网法则；主机到集线器最大距离为 100m；非特别指明，HUB 隐含是指共享式集线器，即双绞线以太网的中继器；因此共享式 10BASE-T 用一层设备组网，最大距离是 500m。

（4）100Mbps 共享式以太网

100Mbps 以太网称为快速以太网，它主要有三个标准规范：

- 100Base-T4：4 对线，cat3 或更高。连线范围 100m。
- 100Base-TX：2 对线，cat5。连线范围 100m。
- 100Base-FX：光纤介质。

如果使用 UTPcat5，其单段连网（不使用连网设备）距离为 100m。使用中继器（共享式 100Mbps 集线器）时，最多允许两个中继器，并且两个中继器之间 UTPcat5 连接长度不超过 5m。即，采用一层设备连网，最大连网范围是 205m。

（5）1000Mbps 共享式以太网

如果使用共享式 1000Mbps 以太网（通信介质 UTPcat5）组网，只能使用一个中继器。单段连网（不使用连网设备）距离为 100m。则最大联网距离为 200m。

实际上，1000Mbps 铜线以太网，一般使用超 5 类和 6 类 UTP 作为通信介质。

参考答案

（29）C

试题（30）

二层以太网交换机联网范围主要受制于__（30）__。

（30）A．MAC 地址　B．CSMA/CD　C．通信介质　D．网桥协议

试题（30）分析

本题主要考查对二层设备工作原理和网桥协议的理解。

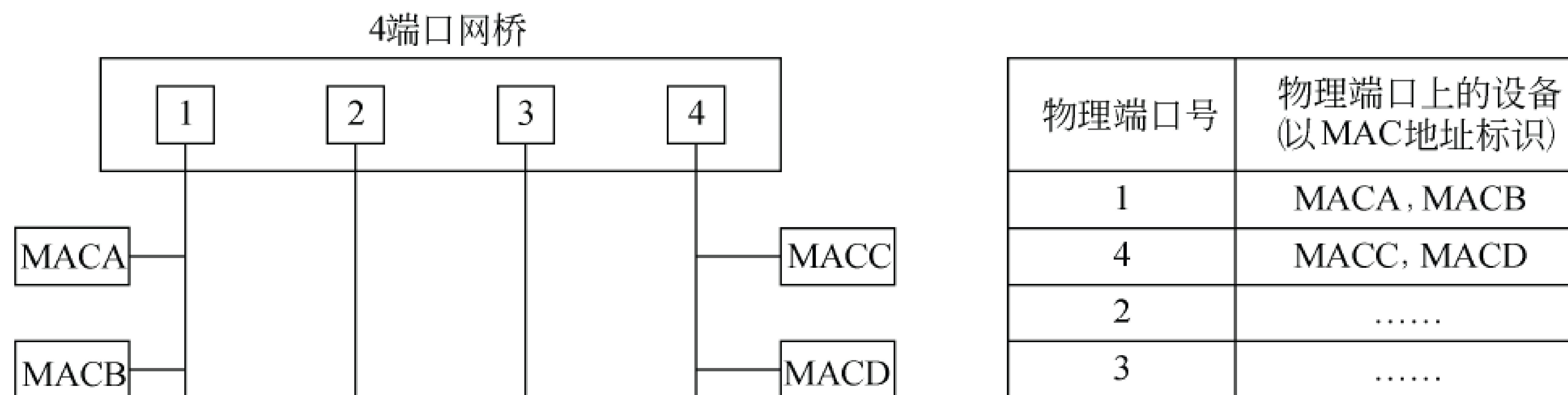
（1）网桥（以以太网为例说明）

网桥是工作在 OSI 协议模型第二层的设备。其和中继器的主要区别是，它根据以太网的帧信息进行以太网帧的转发。在以太网中，传输信息是以以太网帧格式进行传输的。在以太网帧中，包含了 DA——标识目的地址和 SA——标识源地址。以太网帧格式如下。

前导 1010...1010	SFD 10101011	DA	SA	长度	LLC 数据	LLC 填充	FCS
56位	8位	6字节	6字节	2字节	46–1500字节		4字节

802.3 数据包帧格式

网桥设备内部有一个转发表，称为网桥的路由表。表中存有以太网地址（简称 MAC 地址）和网桥物理端口的对应。如下图所示。



物理端口号	物理端口上的设备（以MAC地址标识）
1	MACA，MACB
4	MACC，MACD
2	……
3	……

网桥在物理端口上收到以太网信息后，根据以太网帧中的目的地址，查自己的路由表进行转发。网桥能够区分不同的物理以太网网段，即用中继器互连的以太网。

网桥的转发表是通过自己学习得到的。网桥的每个端口都监听本端口上的所有以太网帧，从监听到的以太网帧的源地址字段得到 MAC 地址和物理端口的对应关系，并填充自己的转发表。

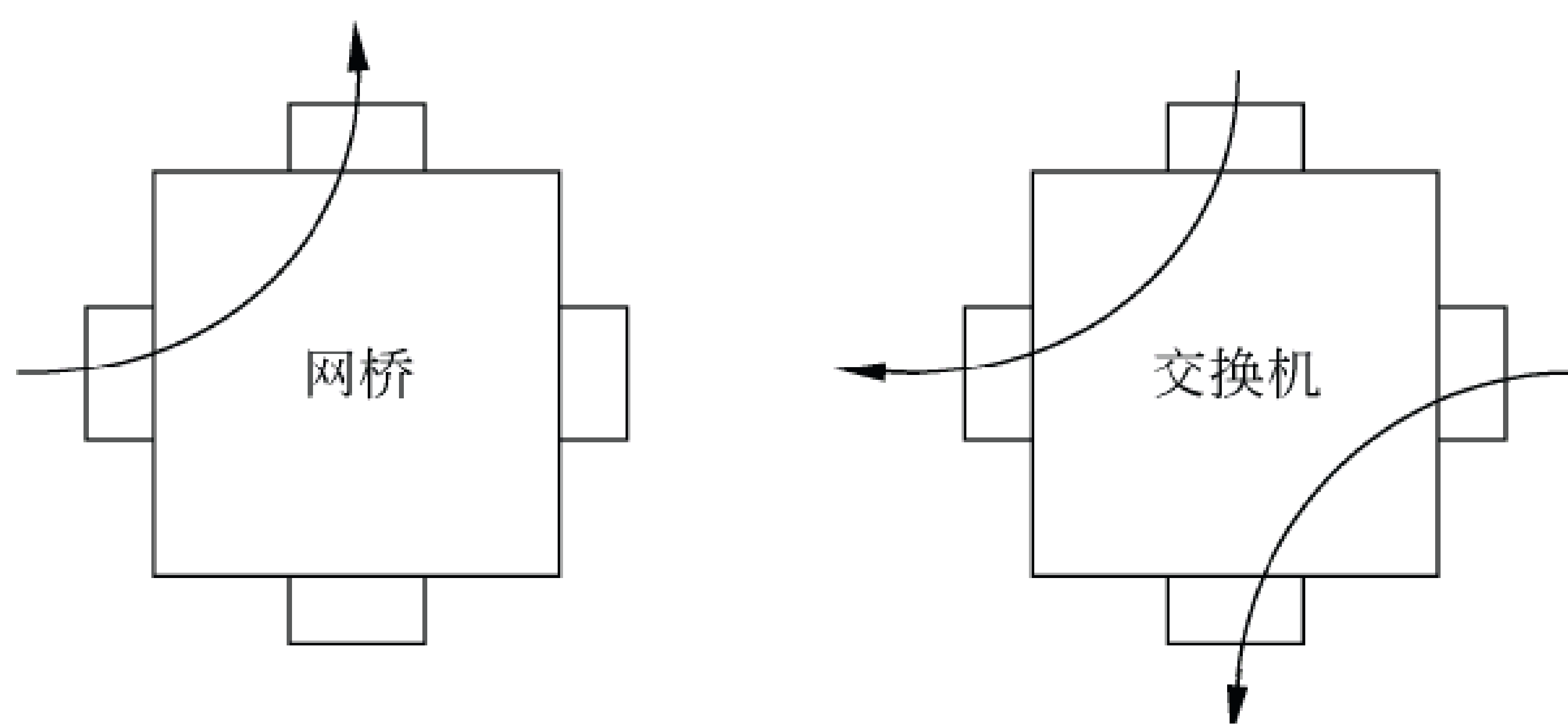
如果有设备同时出现在网桥的两个端口上，则网桥就不能正常工作了，因此用网桥互连的网络不能出现环路。

（2）二层交换设备

二层交换设备本质上也是网桥，工作原理相同，但它是一种功能更强，性能更好的网桥。可以实现多个端口之间同时转发以太网帧。

网桥一般采用软件实现以太网帧的转发，转发数据时，同时只能在两个端口之间进行（无论网桥有多少个端口）。

二层交换，一般指用硬件代替软件进行以太网帧的转发，并且同时能够在交换设备的多个端口之间同时进行转发。下图给出了网桥和交换机的转发差别。



（3）网桥协议

基于网桥的工作原理，用二层设备互连的网络不能有环路。但在实际连网时，我们希望不同网段之间有链路备份，即同一物理连接，具有两个或两个以上的连接通道。这时环路将大量存在。为了解决设备的环路问题，二层设备上必须运行网桥协议。

网桥协议的核心算法是生成树算法。IEEE（电机和电子工程师学会）制定了 802.1D 的生成树协议（Spanning Tree Protocol），它在防止产生环路的基础上提供路径冗余。生成树协议（STP）是通过生成树算法（STA：Spanning Tree Algorithm）计算出一条到根网桥的无环路路径来避免和消除网络中的环路，它是通过判断网络中存在环路的地方并阻断冗余链路来实现这个目的。通过这种方式，它确保到每个目的地都只有唯一路径，不会产生环路，从而达到管理冗余链路的目的。

为了实现对冗余链路的管理，找出存在的冗余链路，STA 在网络中选举根网桥作为依据，跟踪该可用路径。若发现存在冗余路径，它将选择最佳路径来进行数据包转发，并阻断其他冗余链路。

（4）网桥协议的问题和连网距离

STA 运行需要二层设备不断交换链路信息（物理连接的信息），其有信息广播的周期和 STA 算法收敛速度的问题。如果用二层设备组网的规模过大，信息传播和算法收敛将变的不可预测。按经验原则（无理论证明），一般二层设备组网最大可到 7 级左右（7 个二层设备级联）。

参考答案

（30）D

试题（31）

VLAN 实施的前提条件是（31）。

（31）A. 使用 CSMA/CD 协议　　B. 基于二层设备实现

C. 基于二层交换机实现　　D. 基于路由器实现

试题（31）分析

本题考查 VLAN 的概念和实现基础。

VLAN 是在二层实现的，是基于二层交换设备实现的。在普通的网桥上（非交换式）将无法实现 VLAN。

参考答案

（31）C

试题（32）

在以太网半双工共享式连接中，我们无需流量控制；而在全双工交换式连接中要考虑流量控制，其原因是__（32）__。

（32）A. 共享式连接中，由共享式集线器（Hub）完成流量控制

B. 共享式连接中，CD（碰撞检测）起到了拥塞避免的控制机制。全双工中必须附加其他机制来完成

C. 全双工交换式连接带宽扩大了一倍，必须增加流量控制机制

D. 为了在全双工网络中实现 VLAN，必须增加流量控制机制

试题（32）分析

本题考查对 CSMA/CD 和全双工的概念的理解。

共享式或半双工以太网采用带有碰撞检测的载波侦听多路访问（CSMA/CD）的方法进行媒体访问控制。按照这种方法，一个工作站在发送前，首先侦听媒体上是否有活动。所谓活动是指媒体上有无数据传输，也就是载波是否存在。如果侦听到有载波存在，工作站便推迟自己的传输。如果侦听的结果为媒体空闲时，则立即开始进行传输。在侦听到媒体忙时，采用一定的延迟后（有不同的回避策略），可继续检测。如果有两个以上的工作站，同时检测到媒体空闲，同时发送数据，此时就会产生碰撞；每个工作站，在发送数据的同时，也进行碰撞检测，一旦检测到碰撞，将终止当前数据的发送，延迟一定的时间（随机的时间，以减小下次发生碰撞的概率），然后再检测并发送。

从 CSMA/CD 的工作原理看，当用户业务量增大时，碰撞就会增加，此时实际的传输数据量将下降。CSMA/CD 原理的核心是竞争使用传输媒体，其机制本身就能进行流量控制。

全双工交换式连接，将 CSMA/CD 机制中的 CD 取消，同时保证每个物理连接上只有两个设备（点到点连接），这样点到点连接的两个设备可以同时进行数据收发操作。由于缺少了碰撞检测，CSMA 本身无法控制用户的业务流量，全双工交互式连接必须额外增加流控机制来控制用户的业务流量。

参考答案

（32）B

试题（33）

若在一个 IPv4 网络中一共划分了 5 个 VLAN，则该 IPv4 网络中__（33）__。

（33）A. 至少存在 5 个子网　　B. 最多存在 5 个子网
　　C. 至少存在 5 个路由器　　D. 最多存在 5 个路由器

试题（33）分析

本题考查 IP 子网与 VLAN 的映射关系以及 IP 选路原理。请参考试题（12）分析部分。

在 IPv4 网络中，一个 IP 子网只能映射一个 LAN 或 VLAN；多个 IPv4 子网，可以映射到一个 LAN 或 VLAN 中。

同一子网内主机可直接通信；不同子网之间，主机必须通过路由器才能进行通信。

参考答案

（33）A

试题（34）

有一个 IPv4 网络，使用 172.30.0.0/16 网段。现在需要将这个网络划分为 55 个子网，每个子网最多 1000 台主机，则子网掩码是＿（34）＿。

（34）A. 255.255.64.0　　B. 255.255.128.0
　　C. 255.255.224.0　　D. 255.255.252.0

试题（34）分析

本题考查子网划分方法和表示方法。

55 个子网，取最接近的 2 的幂的整数是 64，即 2 的 6 次方

1000 个主机，取最接近的 2 的幂的整数是 1024，即 2 的 10 次方。

即 172.30.0.0/16 的最后 10bit 表示主机 ID，其余为网络 ID。用子网掩码来表示为 255.255.252.0。

参考答案

（34）D

试题（35）、（36）

应用 MPLS VPN 时，针对每个 VPN 地址规划应满足的条件是＿（35）＿。不同的 VPN 信息通过 MPLS 骨干网（或核心网）时通过＿（36）＿进行区分。

（35）A. 每个 VPN 都是独立的，可以使用任何地址，只要保证在 VPN 内部合法正确即可
　　B. VPN 之间的地址不能相互重叠
　　C. VPN 内只能使用公网 IP 地址
　　D. VPN 内只能使用私网 IP 地址

（36）A. IP 地址+AS 号　　B. IP 地址+子网掩码
　　C. VPN 标识符　　D. VPN 标识符+IP 地址

试题（35）、（36）分析

本题考查 VPN 的概念和 MPLS VPN 的工作原理。

（1）VPN 的概念

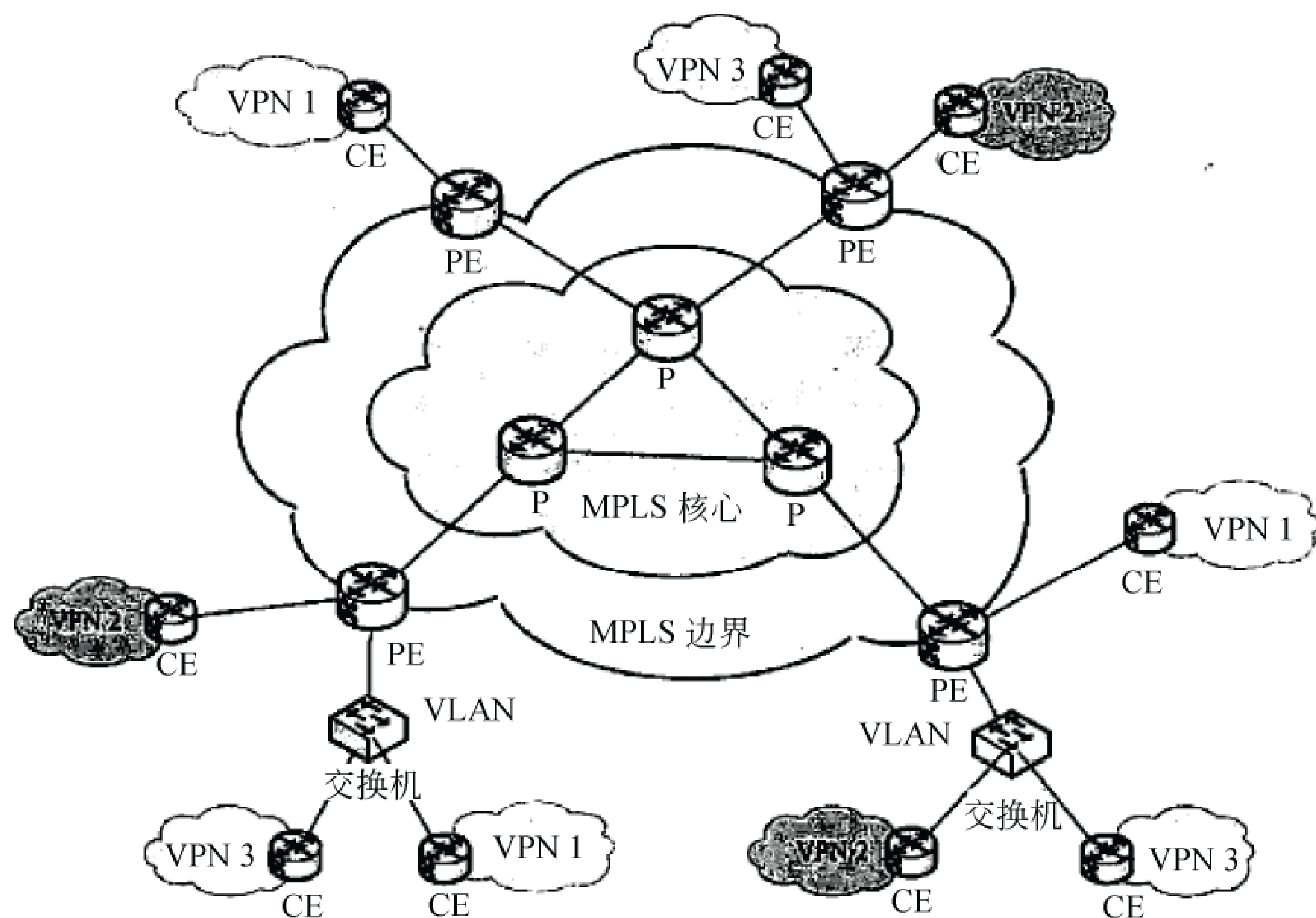
虚拟专用网络（Virtual Private Network，VPN）是建立在公网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而是通过 ISP 提供的公用网络来实现通信，其专用性表现在 VPN 之外的用户无法访问 VPN 内部的资源，VPN 内部用户之间可以实现安全通信。

简单地说，VPN 指在 Internet 上建立的、由用户（组织或个人）自行管理的网络。VPN 的实现是依靠相关技术，在公共的 Internet 上传送专用的、保密的用户私有数据。从用户角度看，VPN 就是自己的专网，只不过，它是通过 VPN 技术在公共的 Internet 网络上虚拟出的网络资源。

（2）MPLS VPN

MPLS VPN 可以基于二层或三层实现。《网络规划设计师教程》中提及的 MPLS VPN 属于 MPLS 三层 VPN。

MPLS 三层 VPN 是一种基于 PE 的 L3VPN 技术。它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。MPLS 三层 VPN 的典型结构如下所示。



MPLS 三层 VPN 模型由三部分组成：CE、PE 和 P。

- CE（Customer Edge）：用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到VPN 的存在，也不需要支持 MPLS。

- PE（Provider Edge）：服务提供商边缘路由器，是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider）：服务提供商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。

MPLS 三层 VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE，因此得到越来越多的应用。

（3）结论

VPN 是用户的专用网络，因此每个 VPN 是独立的。如果每个 VPN 是独立的，就存在地址重叠问题，即两个或多个 VPN 内部的地址信息是重叠的，此时只传递 VPN 内部的路由信息就无法正常进行选路。

要在存在地址重叠的 MPLS 三层 VPN 的 MPLS 骨干（或称核心）网上正确传递 VPN 路由，就必须传递两个信息：VPN 内部的路由信息（用 IP 地址标识）和 VPN 的标识，其中 VPN 标识用于 PE 之间识别要传递到那些 VPN，IP 地址（包括子网标识）用于传递 VPN 内部的路由信息。

参考答案

（35）A　　　（36）D

试题（37）

有一个公司内部网络发生了故障，故障现象是：甲用户可以正常使用内部服务器和互联网服务，乙用户无法使用这些服务。那么检测故障最佳的方法是：<u>（37）</u>。

（37）A. 从乙用户所在的物理网络的物理层开始检查故障，依次检测物理层、数据链路层、网络层直到应用层

B. 从乙用户所在的物理网络的路由器开始检查故障，依次检测路由器，二层交换机、中继器或 HUB

C. 从检测公司的服务器开始，依次检测服务器、网络互联设备、物理层连接

D. 从甲用户所在的物理网络首先开始检测，依次检测物理层、数据链路层、网络层直到应用层

试题（37）分析

本题考查综合的故障检测能力。

在一个公司内部，有人能访问内部服务器和外部服务器，有人不能访问。此时应判断出应用层（对应各种服务）和网络层（外部网络和公司内部网络的公共部分）很有可能是可靠的；而问题很有可能出现在乙用户自己本身或者乙用户所在的网络区域。因此最佳方法是从乙用户的物理层开始检测，依次为物理层、数据链路层、网络层直至应用层。

参考答案

（37）A

试题（38）

某局域网内部有 30 个用户，假定用户只使用 E-mail（收发流量相同）和 Web 两种服务，每个用户平均使用 E-mail 的速率为 1Mbps，使用 Web 的速率是 0.5Mbps，则按照一般原则，估算本局域网的出流量（从局域网向外流出）是＿(38)＿。

（38）A. 45Mbps　　B. 22.5Mbps　　C. 15Mbps　　D. 18Mbps

试题（38）分析

本题考查对通信流量分布的简单规则的掌握和应用

（1）通信流量分布的简单规则

在通信规范分析中，最终的目标是产生通信量，其中必要的工作是分析网络中信息流量的分布问题。在整个过程中，需要依据需求分析的结果来产生单个信息流量的大小，依据通信模式、通信边界的分析，明确不同信息流在网络不同区域、边界的分布，从而获得区域、边界上的总信息流量。

对应部分较为简单的网络，可以不需要进行复杂的通信流量分布分析，仅采用一些简单的方法，例如 80/20 规则、20/80 规则等；但是对于复杂的网络，仍必须进行复杂的通信流量分布分析。

（2）80/20 规则

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：在一个网段中，通信流量的 80%是在该网段内流动，只有 20%的通信流量是访问其他网段。

80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

（3）20/80 规则

随着互联网的发展，一些特殊的网络不断产生，例如小区内计算机用户形成的局域网、大型公司用于实现远程协同工作的工作组网络等。这些网络的特征就是：网段的内部用户之间相互访问较少，大多数对网络的访问，都是对网段外的资源进行访问。对应这些流量分布恰好位于另一个极端，可以采用 20/80 规则。

20/80 规则的思路是：根据对用户和应用需求的统计，产生网段内的通信总量大小，其中 20%的通信流量是在该网段内流动，80%的通信流量是访问外部网段。

80/20 规则和 20/80 规则虽然比较简单，但这些规则是建立在大量的工程经验基础上的；另外通过这些规则的应用，可以很快完成一个复杂网络中大多数网段的通信流量分析工作，可以合理减少大型网络中的设计工作量。

（4）与具体互联网业务相结合

E-mail：发送邮件和接收邮件。视为对等流量，即 50%流出，50%流入。

Web：浏览网络，从 Web 下载的流量大。使用 20/80 法则。流出：20%，流入 80%。

本题答案：流出流量：30×1×50%＋30×0.5×20%＝18Mbps。

参考答案

（38）D

试题（39）、（40）

在采用公开密钥密码体制的数字签名方案中，每个用户有一个私钥，可用它进行＿（39）＿；同时每个用户还有一个公钥，可用于＿（40）＿。

（39）A. 解密和验证　　B. 解密和签名
　　C. 加密和签名　　D. 加密和验证

（40）A. 解密和验证　　B. 解密和签名
　　C. 加密和签名　　D. 加密和验证

试题（39）、（40）分析

本题考查公开密钥密码体制的基础知识。

与只使用一个密钥的对称传统密码不同，公钥密码学是非对称的，它依赖于一个公开密钥和一个与之在数学函数上相关但不相同的私钥。由于公钥可以对外公开，通常用于加密和签名认证（这样与之通信的多个用户可以共用一个加密密钥，密钥管理开销小），私钥是用户自己保管的，通常用于解密和签名。

参考答案

（39）B　（40）D

试题（41）

关于防火墙的功能，下列叙述中哪项是错误的？＿（41）＿。

（41）A. 防火墙可以检查进出内部网络的通信量
　　B. 防火墙可以使用过滤技术在网络层对数据包进行选择
　　C. 防火墙可以阻止来自网络内部的攻击
　　D. 防火墙可以工作在网络层，也可以工作在应用层

试题（41）分析

本题考查防火墙的基础知识。

在建筑上，防火墙被设计用来防止火势从建筑物的一部分蔓延到另一部分，而网络防火墙的功能与此类似，用于防止外部网络的损坏波及到内部网络。其基本工作原理是在可信任网络的边界（即常说的在内部网络和外部网络之间，通常认为内部网络是可信任的和安全的，而外部网络是不可信的和不安全的）建立起访问控制系统，隔离内部和外部网络，执行访问控制策略，防止外部的未授权结点访问内部网络和非法向外传递内部信息。防火墙一般安放在被保护网络的边界，只有在所有进出被保护网络的通信都通过防火墙的情况下，防火墙才能起到安全防护作用。

如果针对内部网络的攻击是来自网络内部的话，其相关通信数据不会经过防火墙，则防火墙的访问控制安全策略不能对攻击通信数据加以检查和控制，所以防火墙不能阻止来自网络内部的攻击。也就是说防火墙只能防“外贼”不能防“内贼”。

参考答案

（41）C

试题（42）

以下哪种技术不是实现防火墙的主流技术？__（42）__。

（42）A. 包过滤技术　　B. NAT 技术
C. 代理服务器技术　　D. 应用级网关技术

试题（42）分析

本题考查实现防火墙主要技术的基础知识。

防火墙技术可根据防范的方式和侧重点的不同分为：包过滤型技术、应用级网关技术和代理服务器技术三种类型。

NAT（Network Address Translation，网络地址转换）是一种将私有（保留）地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。NAT 技术在解决 IP 地址不足的同时，能隐藏并保护网络内部的计算机，从而能有效地避免来自网络外部的攻击，通常同防火墙技术配合使用。但是它本身不是实现防火墙的技术。

参考答案

（42）B

试题（43）

PKI 的基本组件不包括以下哪个部分？__（43）__。

（43）A. 注册机构 RA　　B. 认证机构 CA
C. 证书库　　D. 公开可访问的目录

试题（43）分析

本题考查 PKI（Public Key Infrastructure，公钥基础设施）的系统组成的基础知识。

PKI 是一个采用公钥理论和技术来提供安全服务的具有普适性的安全基础设施，是网络安全建设的基础及核心。PKI 采用证书来进行公钥管理，其主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而有效地保护通信数据的机密性、完整性和有效性。

一个典型的 PKI 系统框架通常包括注册机构 RA、认证机构 CA 和证书发布系统。其中认证机构 CA 负责管理公钥的整个生命周期，其作用包括发放证书、规定证书的有效期和发布证书废除列表；注册机构 RA 提供用户和 CA 之间的一个接口，主要完成收集用户信息和确认用户身份的功能；证书发布系统负责证书的集中存放，用户可以从此处获得其他用户的证书和公钥，一般采用证书库或目录服务。“公开可访问的目录”有迷惑的效果，但是并不等同于目录服务。

参考答案

（43）D

试题（44）

以下哪项功能电子签名（electronic signature）不能提供：（44）。

（44）A. 电子文件的保密性
B. 电子文件的完整性
C. 能鉴别文件签署者的身份
D. 文件签署者同意电子文件的内容

试题（44）分析

本题考查电子签名技术的基础知识。

电子签名具有法律效用。从技术的角度，电子签名以电子形式存在，依附于电子文件并与其逻辑关联，可用以识别电子文件签署者身份，保证文件在传输过程中没有受到破坏（即保证电子文件的完整性），并表示签署者同意电子文件的内容。

保密性和完整性不是同一个概念，保密性要求信息不被泄露给未授权的人，完整性要求信息会受到各种原因的破坏。电子文件的保密性通常需要由加密技术来提供。电子签名技术和加密技术是相互独立的，虽然两者经常结合起来使用。

参考答案

（44）A

试题（45）

企业主页上的内容是提供企业的相关消息供大家访问，这时不需要保护消息的（45）。

（45）A. 可靠性　B. 完整性
C. 保密性　D. 真实性

试题（45）分析

本题考查网络安全的基础知识。

保密性是指信息泄露给非授权用户/实体/过程从而被非法利用；完整性指未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失；可靠性指系统能正常工作不出故障；真实性指信息的来源是真实的或身份是真实的。

企业主页上的内容是公开给所有人看的，也就是说所有人都是合法授权用户，因此不需要采用措施来保证保密性。

参考答案

（45）C

试题（46）

小王在安装基于 UNIX 的服务器系统时想给系统增加安全审计功能，最简便的做法是（46）。

（46）A. 启动和配置 UNIX 操作系统的各种系统日志功能
B. 安装 NetSC 日志审计系统

C. 安装防火墙

D. 安装入侵检测系统

试题（46）分析

本题考查安全审计的基础知识。

安全审计包括识别、记录、存储、分析与安全相关行为的信息。对于计算机系统，这些信息通常保持在系统日志中。因此如果想增加 UNIX 的服务器系统的安全审计功能，只需启动和配置 UNIX 操作系统的各种系统日志功能，就能在系统日志中保存同审计相关的数据。

参考答案

（46）A

试题（47）

关于加密技术，下面哪种说法是错误的？__（47）__。

（47）A. 为提高安全性，密码体制中加密算法和解密算法应该保密

B. 所有的密钥都有生存周期

C. 密码分析的目的就是千方百计地寻找密钥或明文

D. 公开密钥密码体制能有效地降低网络通信中密钥使用的数量

试题（47）分析

本题考查密码体制的基础知识。

对于一个好的密码体制，其安全强度应该不依赖于密码体制本身（包括明文的统计特性、加密操作方式、处理方法和加/解密算法 、密钥空间及其统计特性等）的保密，而只依赖于密钥。

参考答案

（47）A

试题（48）

某公司的人员流动比较频繁，网络信息系统管理员为了减少频繁的授权变动，其访问控制模型应该采用__（48）__。

（48）A. 自主型访问控制　　B. 强制型访问控制

C. 基于角色的访问控制　　D. 基于任务的访问控制

试题（48）分析

本题考查访问控制技术的基础知识。

访问控制是指主体依据某些控制策略或权限对客体本身或是资源进行的不同授权访问。访问控制包括三个要素：主体、客体和控制策略。访问控制模型是一种从访问控制的角度出发，描述安全系统，建立安全模型的方法。访问控制模型通常分为自主型访问控制模型、强制型访问控制模型、基于角色的访问控制模型、基于任务的访问控制模型和基于对象的访问控制模型。

自主型访问控制模型的特点是授权的实施主体自主负责赋予和回收其他主体对客体资源的访问权限；强制型访问控制模型的特点是系统对访问主体和受控对象实施强制访问控制，主体和客体都被分配了一个固定安全属性，根据主体/客体的安全属性决定主体是否能够访问客体；基于角色的访问控制模型的特点是访问控制由各个用户在部门中所担任的角色来确定，而不是基于员工在哪个组或谁是信息的所有者；基于任务的访问控制模型的特点是以从任务（活动）的角度来建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。

本题中给出的条件是公司的人员流动比较频繁，但是公司中的角色（职位）一般是不会变化，因此适合采用基于角色的访问控制模型。

参考答案

（48）C

试题（49）、（50）

用 IPSec 机制实现 VPN 时，如果企业内部网使用了私用 IP 地址，应该采用<u>（49）</u>技术，IPSec 该采用<u>（50）</u>模式。

（49）A. NAT 技术　　B. 加密技术

C. 消息鉴别技术　　D. 数字签名技术

（50）A. 传输模式　　B. 隧道模式

C. 传输和隧道混合模式　　D. 传输和隧道嵌套模式

试题（49）、（50）分析

本题考查 VPN 和 IPSec 的基础知识。

VPN 的目标是在不安全的公共网络上建立一个安全的专用通信网络，通常采用加密和认证技术，利用公共通信网络设施的一部分来发送专用信息，为相互通信的结点建立起的一个相对封闭的、逻辑上的专用网络。构建 VPN 需要采用“隧道”技术，建立点对点的连接，使数据包在公共网络上的专用隧道内传输。

在 IPSec 协议中有两种工作模式：传输模式和隧道模式。这两种模式的区别非常直观——它们保护的对象不同，传输模式保护的是 IP 载荷，而隧道模式保护的是整个 IP 包。

由于企业内部网使用了私用 IP 地址，必须通过 NAT 转换为公网地址才能与外界通信。同时由于是搭建 VPN，IPSec 应该工作在隧道模式才能建立起 VPN 所需的隧道。

参考答案

（49）A　（50）B

试题（51）

关于入侵检测系统的描述，下列叙述中哪项是错误的？<u>（51）</u>。

（51）A. 监视分析用户及系统活动

B. 发现并阻止一些已知的攻击活动

C. 检测违反安全策略的行为

D. 识别已知进攻模式并报警

试题（51）分析

本题考查入侵检测系统的基础知识。

入侵检测系统是通过从计算机网络和系统的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定的措施的系统。

入侵检测系统的目标在检测和发现攻击活动，自身并不能阻止攻击活动。只有与防火墙等设备联动，才有可能阻止一些攻击活动。

参考答案

（51）B

试题（52）

AH 协议中用于数据源鉴别的鉴别数据（ICV）是由 IP 分组中的校验范围内的所有 “固定” 数据进行计算得到的，以下哪个数据不在计算之列？（52）。

（52）A. IP 分组头中的源 IP 地址

B. IP 分组头中的目的 IP 地址

C. IP 分组头中的头校验和

D. IP 分组中的高层数据

试题（52）分析

本题考查 IPSec 协议中的 AH 协议的基础知识。

AH 协议中用于数据源鉴别的鉴别数据（ICV）是由 IP 分组中的校验范围内的所有“固定”数据进行计算得到的，也就是说原 IP 数据包头中不变的或接受端可预测的字段都会在安全保护范围之内，如果在传输过程中发生改变，则 ICV 也会发生改变。

4 个选项中“IP 分组头中的头校验和”选项会随着其他一些可变字段（如存活时间 TTL 等）的变化而变化，不属于固定数据，故不在计算之列。

参考答案

（52）C

试题（53）

特洛伊木马程序分为客户端（也称为控制端）和服务器端（也称为被控制端）两部分，当用户访问了带有木马的网页后，木马的（53）部分就下载到用户所在的计算机上，并自动运行。

（53）A. 客户端 B. 服务器端

C. 客户端和服务器端 D. 没有

试题（53）分析

本题考查特洛伊木马程序的基础知识。

对木马程序而言，它一般包括两个部分：客户端（控制端）和服务器端（被控制端）。

服务器端安装在被控制的计算机中，一般通过电子邮件或其他手段让用户在其计算机中运行，以达到控制该用户计算机的目的。客户端程序是控制者所使用的，用于对受控的计算机进行控制。服务器端程序和客户端程序建立起连接就可以实现对远程计算机的控制。

参考答案

（53）B

试题（54）

以下哪种程序不属于恶意代码？<u>（54）</u>。

（54）A. widget　　B. 特洛伊木马
C. 僵尸程序　　D. 网络蠕虫

试题（54）分析

本题考查恶意代码的基础知识。

恶意代码指未经用户授权而干扰或破坏计算机系统/网络的程序或代码。恶意代码通常具有如下共同特征：具有恶意的目的；自身是计算机程序；通过执行发生作用。一般分为特洛伊木马、僵尸程序、网络蠕虫、计算机病毒、间谍软件和垃圾邮件等。

widget 指能够面向最终用户独立运行的功能实体，一般来讲根据运行位置的不同可以分为 Web Widget、桌面 Widget 和移动 Widget 等，它的表现形式可能是视频，地图，新闻，小游戏等等，Widget 是当前非常流行的一项技术，能够极大地方便用户的桌面应用和网络应用。它的根本思想来源于代码复用，不具有恶意的目的。

参考答案

（54）A

试题（55）～（61）

黑客小张一天想尝试入侵某公司网络，窃取机密信息。为提高效率，他需要做的第一步工作通常是<u>（55）</u>；第二步通常是<u>（56）</u>；在成功入侵该公司网络某台主机并取得该主机的控制权后，通常所做的工作是<u>（57）</u>；在窃取到机密信息后，最后需要做的工作是<u>（58）</u>；为了预防黑客入侵的第一步，该公司网络应该采取的预防措施为<u>（59）</u>；针对第二步的预防措施为<u>（60）</u>。为了能及时发现上述入侵，该公司网络需要配备<u>（61）</u>。

（55）A. 收集目标网络的所在位置及流量信息
B. 到网上去下载常用的一些攻击软件
C. 捕获跳板主机，利用跳板主机准备入侵
D. 通过端口扫描等软件收集目标网站的 IP 地址、开放端口和安装的软件版本等信息

（56）A. 了解目标网络的所在位置的周围情况及流量规律，选择流量小的时间

发起攻击

B. 下载攻击软件，直接发起攻击

C. 向目标网络发起拒绝服务攻击

D. 根据收集的开放端口和安装的软件版本等信息，到网络查找相关的系统漏洞，下载相应的攻击工具软件

（57）A. 修改该主机的 root 或管理员口令，方便后续登录

B. 在该主机上安装木马或后门程序，方便后续登录

C. 在该主机上启动远程桌面程序，方便后续登录

D. 在该主机上安装网络蠕虫程序以便入侵公司网络中的其他主机

（58）A. 尽快把机密数据发送出去

B. 在主机中留一份机密信息的副本，以后方便时来取

C. 删除主机系统中的相关日志信息，以免被管理员发现

D. 删除新建用户，尽快退出，以免被管理员发现

（59）A. 尽量保密公司网络的所在位置和流量信息

B. 尽量减少公司网络对外的网络接口

C. 尽量关闭主机系统上不需要的服务和端口

D. 尽量降低公司网络对外的网络接口速率

（60）A. 安装网络防病毒软件，防止病毒和木马的入侵

B. 及时对网络内部的主机系统进行安全扫描并修补相关的系统漏洞

C. 加大公司网络对外的网络接口速率

D. 在公司网络中增加防火墙设备

（61）A. 入侵检测系统

B. VPN 系统

C. 安全扫描系统

D. 防火墙系统

试题（55）～（61）分析

本题考查黑客攻击及防御的基础知识。

黑客攻击的典型攻击步骤如下：1）信息收集，信息收集在攻击过程中的位置很重要，直接影响到后续攻击的实施，通常通过扫描软件等工具获取被攻击目标的 IP 地址、开放端口和安装的软件版本等信息；2）根据收集到的相关信息，去查找对应的攻击工具；3）利用查找到的攻击工具获得攻击目标的控制权；4）在被攻破的机器中安装后门程序，方便后续使用；5）继续渗透网络，直至获取机密数据；6）消灭踪迹，消除所有入侵脚印，以免被管理员发觉。

针对上述的攻击过程，需要尽量关闭主机系统上不需要的服务和端口防止黑客收集到相关信息，同时需要及时对网络内部的主机系统进行安全扫描并修补相关的系统漏洞

以抵御相应攻击工具的攻击。为了能及时发现上述入侵，需要在关键位置部署 IDS。

参考答案

（55）D　（56）D　（57）B　（58）C　（59）C　（60）B　（61）A

试题（62）、（63）

网络安全应用协议 SSL 协议工作在（62），HTTPS 协议工作在（63）。

（62）A. 数据链路层　B. 网络层　C. 传输层　D. 应用层

（63）A. 数据链路层　B. 网络层　C. 传输层　D. 应用层

试题（62）、（63）分析

本题考查网络安全应用协议的基础知识。

SSL（Secure Sockets Layer，安全套接层）的设计目标是在 TCP 基础上提供一种可靠的端到端的安全服务，其服务对象一般是 Web 应用。它指定了一种在应用层协议和 TCP/IP 协议之间提供数据安全性分层的机制，因此它工作在传输层。这个协议的第三版 SSLv3 经过改进后被 IETF 的 TLS 工作组接受作为传输层安全协议（Transport Layer Security，TLS）。

HTTPS（Hypertext Transfer Protocol over Secure Socket Layer，基于 SSL 协议的 HTTP），提供了身份验证与加密通信方法，用于安全的 HTTP 数据传输，因此它工作在应用层。

参考答案

（62）C　（63）D

试题（64）

在实施网络规划项目时，创建项目工作分解结构的作用是（64）。

（64）A. 协调项目利益相关者的要求

B. 确认项目经理并进行授权

C. 分析项目涉及的工作，明确项目任务范围

D. 监测项目的成本执行情况以衡量项目绩效

试题（64）分析

本题考查项目范围管理方法“工作分解结构（WBS）”的基本知识。

工作分解结构是一种以结果为导向的分析方法，用于分析项目所涉及的工作，所有这些工作构成了项目的整体范围。工作分解结构是计划和管理项目进度、成本和变更的基础，是项目管理中一个非常基本的文件。因此，创建项目工作分解结构的作用是分析项目涉及的工作，明确项目任务范围。

参考答案

（64）C

试题（65）

在对项目中某项活动所耗费的时间进行估算时，可给出三个时间估计：乐观时间 t_o、

悲观时间 t_p 和最可能时间 t_m，则该项活动的期望工期为__（65）__。

（65）A. $\frac{t_o + t_m + t_p}{3}$　　B. $\frac{t_o + 2t_m + t_p}{4}$

C. $\frac{t_o + 3t_m + t_p}{5}$　　D. $\frac{t_o + 4t_m + t_p}{6}$

试题（65）分析

本题考查项目管理中活动历时估计方法的基本知识。

在对项目中要完成的各项活动的历时进行估计时，当存在高度不确定因素时，可采用概率时间估计法，对活动确定三个估计时间，即：乐观时间 t_o、最可能时间 t_m 和悲观时间 t_p。采用三个时间估计时，是假定三个估计均服从 β 概率分布，在这个假定的基础上，活动的期望工期可以用公式 $\frac{t_o + 4t_m + t_p}{6}$ 计算。

参考答案

（65）D

试题（66）

在项目成本管理中，估算完成项目所需资源总成本的方法不包括__（66）__。

（66）A. 类比法　　B. 甘特图法　　C. 参数模型法　　D. 自下而上累加法

试题（66）分析

本题考查项目管理中成本估算方法的基本知识。

项目的成本估算需要给出完成项目所需资源成本的近似值。成本估算的主要技术包括：类比估算法、自下而上估算法和参数模型估算法。类比估算法是使用以前相似项目的实际成本作为目前项目成本估算的根据；参数模型法是应用项目特征参数建立数学模型来估算成本；自下而上累加法是在工作分解结构的基础上，分别估算每个工作包的成本，然后自下而上将所有的估算相加，最终完成整个项目的估算。而甘特图法是进行项目进度管理的最常用的工具，其通常形式是纵向表示项目的各项工作，横向表示所需的时间，不具备成本估算的功能。

参考答案

（66）B

试题（67）

根据《中华人民共和国著作权法》和《计算机软件保护条例》的规定，对于法人或其他组织的软件著作权，保护期为__（67）__。

（67）A. 20 年　　B. 30 年　　C. 50 年　　D. 70 年

试题（67）分析

本题考查软件相关知识产权保护法规的基础知识。

《计算机软件保护条例》规定：软件著作权属于软件开发者，软件著作权自软件开发完成之日起产生。自然人的软件著作权，保护期为自然人终生及其死亡后 50 年，法人或者其他组织的软件著作权，保护期为 50 年。

参考答案

（67）C

试题（68）

项目每个阶段结束时的一个重要工作是进行项目绩效评审，评审的主要目标是（68）。

（68）A. 决定项目是否能够进入下一个阶段
B. 根据过去的绩效调整项目进度和成本基准
C. 评定员工业绩和能力
D. 得到客户对项目绩效认同

试题（68）分析

本题考查项目管理中有关项目生命周期管理的基础知识。

由于项目具有一定的不确定性，将一个项目划分为若干阶段，是有效实施管理与控制的常用做法。例如，可将项目生命周期划分为项目定义、项目开发、项目实施、项目收尾四个阶段。对于每个阶段应明确工作目标和任务，在每个阶段结束时，要对该阶段的绩效进行评审，检验阶段目标达成情况，及时发现和解决其中存在的问题，避免将问题带入下一个阶段，只有通过了阶段绩效评审，项目才能够进行下一个阶段。

参考答案

（68）A

试题（69）

在对规划项目进行经济效益评价时，常使用净现值、净现值率、投资回收期、内部收益率等评价指标。当（69）时，规划项目具有经济可行性。

（69）A. 净现值大于 0
B. 投资回收期大于行业基准投资回收期
C. 内部收益率小于行业的基准收益率
D. 折现率大于行业基准收益率

试题（69）分析

本题考查项目经济效益评价主要指标的含义和评价标准。

净现值是指按行业基准收益率或设定的折现率，将项目计算期内各年净现金流量折现到建设期初的现值之和。该指标表示项目在整个寿命期内所取得的净收益的现值，如果净现值大于 0，说明项目能够盈利、具有经济可行性；如果净现值小于 0，说明项目不具有经济可行性。

净现值率是项目净现值与项目总投资现值之比，常用于多方案比较，能够反映资金

的利用效率。

投资回收期是指以项目的净收益抵偿全部投资所需要的时间。投资回收期越短说明项目盈利能力越强。在项目评价中，要将计算出的项目投资回收期与行业的基准投资回收期进行比较，前者小于后者时，表明项目能在规定的时间内收回投资，否则项目不具备经济可行性。

内部收益率是指项目在整个计算期内各年净现金流量现值累计等于零时的折现率，它反映了项目以每年的净收益归还全额投资以后，所能获得的最大收益率。只有当内部收益率大于行业的基准收益率时，项目才具备经济可行性。

折现率本身并不是评价指标，而是用于计算净现值、动态投资回收期等指标的参数，可预先设定，或取定为行业基准收益率。

参考答案

（69）A

试题（70）

某企业拟建设通信网络对外提供服务。根据市场预测，未来业务发展好的概率为 0.7，业务发展差的概率为 0.3。现有三种规划方案可供选择：

方案 1，直接投资 3000 万元大规模建网。若业务发展得好，每年可获利 1000 万元，若业务发展不好，每年亏损 200 万元，服务期为 10 年；

方案 2，投资 1400 万元建设小规模网络。若业务发展得好，每年可获利 400 万元，若业务发展不好，每年仍可获利 300 万元，服务期为 10 年；

方案 3，前 3 年按方案 2 实施，即先投资 1400 万元建设小规模网络，收益同方案 2。3 年后若业务发展不好，则继续按方案 2 实施；若业务发展得好，则再追加投资 2000 万元进行网络扩容，扩容后服务期为 7 年，每年可获利 950 万元。

根据以上条件经计算可知<u>（70）</u>。

（70）A. 方案 1 的期望净收益为 5000 万元

B. 方案 3 的期望净收益为 3595 万元

C. 方案 1 为最优方案

D. 方案 2 为最优方案

试题（70）分析

本题考查风险型决策方法和概率相关的基础知识。

在风险型决策问题中，各种方案的实施在不同的条件下所导致的后果是不一样的，而各种条件和后果出现的概率是可以测算的，决策者可以通过计算出各方案在不同条件下的期望收益来考虑未来的经济效果。针对本题分别计算三种方案的期望净收益，期望净收益最大的为最优方案。

该方案 1 的期望净收益为：

$[0.7\times1000+0.3\times(-200)]\times10-3000=3400$（万元）。

方案 2 的期望净收益为：

(0.7×400+0.3×300)×10–1400=2300（万元）。

方案 3 的期望净收益为：

0.7×(400×3–2000+950*7)+0.3×300×10–1400=3595（万元）。

计算结果表明，方案 3 的期望净收益最大，因此，方案 3 为最优方案。

参考答案

（70）B

试题（71）～（75）

A glue that holds the whole Internet together is the network layer protocol, (71). Unlike most older network layer protocols, it was designed from the beginning with internetworking in mind. Its job is to provide a (72) way to transport datagrams from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between them.

Communication in the Internet works as follows. The (73) layer takes data streams and breaks them up into datagrams. Each datagram is transmitted through the Internet, possibly being fragmented into smaller units as it goes. When all the pieces finally get to the destination machine, they are reassembled by the (74) layer into the original datagram. This datagram is then handed to the transport layer, which inserts it into the receiving process' input stream.

An IP datagram consists of a header part and a text part. The header has a (75) part and a variable length optional part.

（71）A. IP (Internet Protocol)
B. IP (Interworking Protocol)
C. TCP (Transport Control Protocol)
D. TCP (Transfer Communication Protocol)

（72）A. best-quality　B. quality-guaranteed
C. connection-oriented　D. best-efforts

（73）A. data link　B. transport
C. network　D. application

（74）A. data link　B. transport
C. network　D. application

（75）A. 40-byte fixed　B. 64-byte fixed
C. 20～64 bytes variable　D. 20-byte fixed

参考译文

将整个互联网连成一体的是网络层协议（71）。与大多数更早的网络层协议不同，

它在设计之初就充分考虑了网络互连。它负责提供一种（72）的方式，从信源到信宿传递数据报，不管信源和信宿机器是否在同一个网络中，或者它们之间是否有其他网络。

互联网中的通信遵照以下方式进行。（73）层将数据流分割成数据报，每个数据报通过互联网传输的过程中，有可能被分割成更小的单元。当所有的数据单元最终到达目的地主机时，它们被（74）层重新组合成原始数据报。这个数据报随后被提交给传输层，由传输层将其插入接收进程的输入流中。

一个 IP 数据报包含报头和报文两部分。报头包括一个（75）部分和一个可变长度的可选部分。

参考答案

（71）A （72）D （73）B （74）C （75）D

第 11 章　2011 下半年网络规划设计师下午试卷 I 试题分析与解答

试题一（30 分）

阅读下列有关企业发展和企业网络建设的说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

某企业最初只有一个办公地点，所有人员都集中在一个相对较小的封闭空间进行工作。由于是小型企业，社会影响不大，所以对安全性要求不高，主要目标是以最小的代价（费用）实现联网和访问互联网（Internet），企业内部无对外提供的任何互联网服务。后来，随着企业不断发展，其网络建设也不断升级更新。（注：以下问题均不考虑无线网络技术）

【问题 1】（10 分）

假定初期员工不超过 50 人，所有员工工作在同一楼层的不同房间，对互联网的访问带宽需求小于 2Mbps，且主要为进入企业内部的流量。

针对该企业网络建设，请从下面几个方面简要说明网络设计内容及依据：（1）网络结构；（2）物理层技术选择；（3）局域网技术选择；（4）广域网技术选择；（5）网络地址规划。

【问题 2】（10 分）

假定企业发展为中等规模，人数不超过 1000 人，所有员工在同一城市的不同地域工作。企业目前分为一个总部和三个分部（分布范围都不超过 2km），总部人数不超过 400 人，分部人数不超过 200 人。企业与互联网采用统一对外接口，带宽需求规模为 100Mbps 以内，且流入数据量和流出数据量基本均衡；企业总部和分部之间的数据流量小于 1000Mbps。由于企业规模较大，对网络的依赖度大大增加，要求分部到总部和总部至互联网出口有备份，以增加网络的健壮性和可用性。

请从下面 3 个方面简要给出总部/分部网络和企业整体网络的结构和设计要点：（1）网络结构；（2）物理层和局域网技术选择；（3）接入互联网技术选择。

【问题 3】（10 分）

如果企业规模扩大到 10000 人，需要对外提供互联网服务（服务器的域名与 IP 一一对应），对内提供企业内部服务，并允许员工访问互联网。假定企业总部和分部数量有 50 个，总部最多 500 人，分部最多 400 人。企业组织机构有 10 个（如行政管理、生产、销售等），每个机构在总部或单个分部最多 60 人。

（1）请简要分析该企业网络的网络地址类型及规模。

（2）考虑管理便利、信息相互隔离和路由聚合等因素，请说明应如何规划该企业网络的子网层次。

（3）举例说明如何进行子网划分（子网划分举例必须能够看出子网划分的规律，至少给出三个以上的子网号）。

试题一分析

网络规划与设计过程一般会经历需求分析、逻辑网络设计、物理网络设计、规划及实施阶段。本题重点考查需求分析、逻辑网络设计这两个方面。

逻辑网络设计工作包括：网络结构设计；物理层技术选择；局域网技术选择；广域网技术选择；地址设计与命名模型；路由选择协议；网络管理；网络安全和逻辑网络设计文档。在逻辑网络设计方面，本题侧重考查网络结构设计、局域网技术选择、广域网技术选择、网络地址规划以及可扩展性网络结构设计方面的问题。

（1）逻辑网络设计原则

根据用户需求设计逻辑网络，选择正确的网络技术比较关键，在选择时应考虑如下因素：

- 通信带宽

所选择的网络技术必须保证足够的带宽，能够为用户访问应用系统提供保障；在进行选择时，不能仅局限于现有的应用要求，还要考虑适当的带宽增长需求。

- 技术成熟度

所选择的网络技术必须是成熟稳定的技术，有些新的应用技术在尚没有大规模投入应用时，还存在着较多的不确定因素，而这些不确定因素可能会为网络的建设带来很多不可估量的损失。虽然新技术的自身发展离不开工程应用，但是对于大型网络工程来说，项目本身不能成为新技术的实验田；因此，使用较为成熟、拥有较多案例的技术是明智的选择。

当然，在面对技术变革时，可采用试点的方式逐步应用。

- 连接服务类型

连接服务类型是逻辑设计时必须考虑的问题，传统的连接服务分为面向连接服务与非连接服务，逻辑设计需要在无连接和面向连接的协议之间进行权衡。

互联网采用 TCP/IP 协议簇，其网络层协议是 IP 协议，提供无连接的服务，因此选择连接服务类型，主要是针对 IP 协议底层的承载协议进行选择。如果选择面向连接服务类型，则可以选择 ATM、SDH 等协议；如果选择非连接服务类型，则可以选择以太网等协议。不同的网络工程，对连接服务类型的需求不同，设计者不能仅局限于一种连接服务而进行设计。

- 可扩展性

网络设计者的设计依据是较为详细的需求分析，但是在选择网络技术时，不能仅考虑当前的需求，而忽视未来的发展；在大多数情况下，设计人员都会在设计中预留一定

的冗余，无论是在带宽、通信容量、数据吞吐量、用户并发数等方面，网络实际需求和设计目标之间的比例应小于一个特定值以便于未来的发展；一般来说，这个值介于 70%～80%之间，在不同的工程中，可根据需要进行调整。

- 高投资产出

选择网络技术的最关键一条，不是技术的扩展性、高性能，也不是成本最低等概念，决定设计和网络管理人员采用某种技术的最关键点是技术的投入产出比，只有通过投入产出分析，才能最后决定技术的使用。

（2）网络结构设计

网络结构是对网络进行逻辑抽象，描述网络中的主要连接设备和计算机结点分布而形成的网络主体框架。网络结构和网络拓扑结构的最大区别在于：网络拓扑结构中，只有点和线，不会出现任何的设备和计算机结点；网络结构主要是描述连接设备和计算机结点的连接关系。

由于当前的网络主要由局域网和实现局域网互联的广域网构成，因此可以将网络工程中的网络结构设计分为局域网结构和广域网结构两个设计部分，其中局域网结构主要关注数据链路层的设备互连方式；广域网结构主要关注网络层设备的互连方式。

（3）局域网结构

- 单核心局域网结构

由一台核心三层交换机设备为中心构建的一种局域网结构，计算机结点通过多台接入交换机接入核心。整个局域网通过核心交换机与公共的互联网相连。

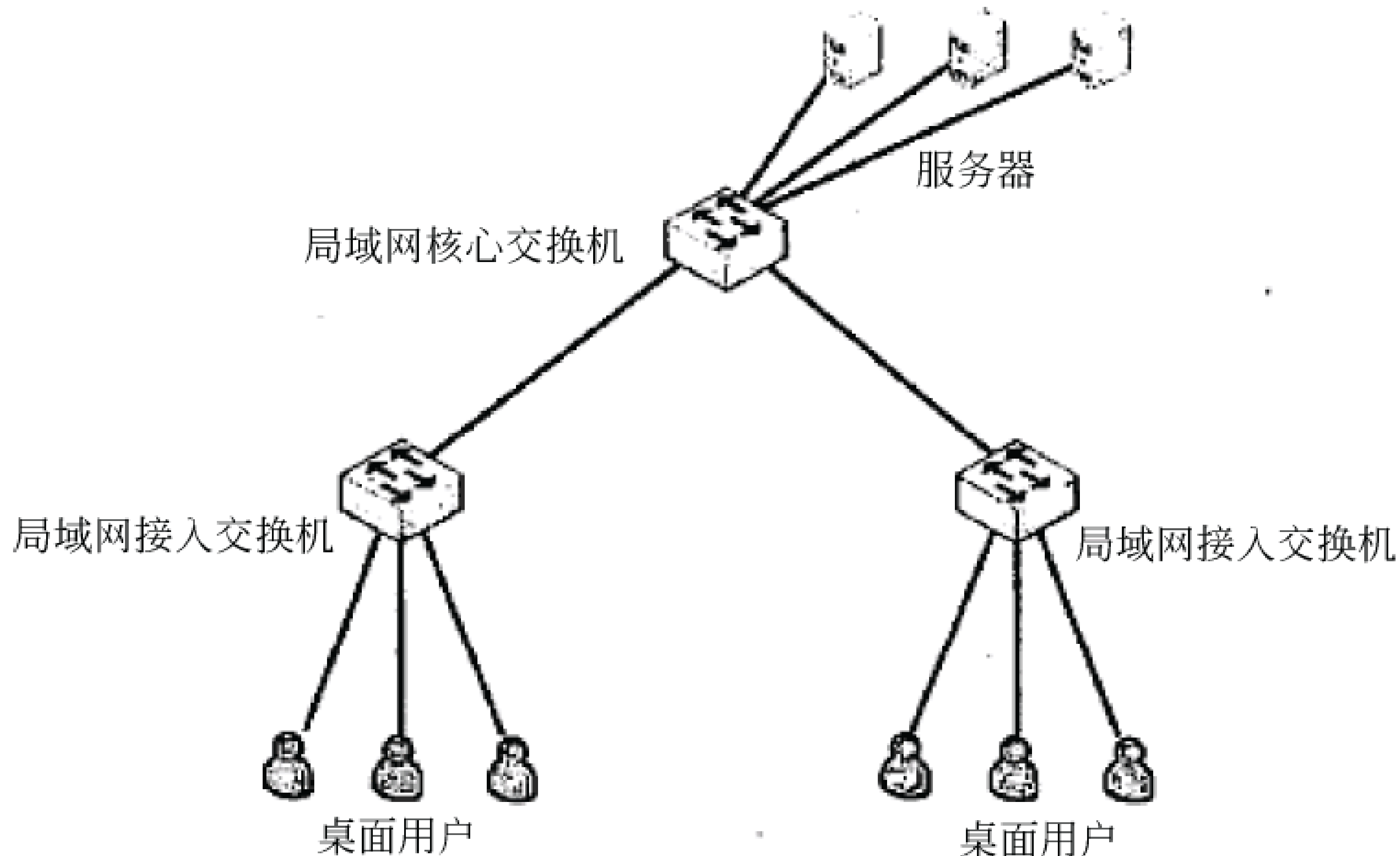


图 1-1　单核心局域网结构

- 单核心结构局域网的主要特点：
  - ➢ 一台核心交换设备，路由功能只存在于核心设备上；

- ➢ 结构简单，管理维护方便；
- ➢ 投资小；
- ➢ 网络覆盖范围小，要求网络分布比较紧凑；
- ➢ 核心设备故障将导致网络瘫痪；
- ➢ 可扩展为双核心局域网结构或层级结构的局域网。

- 双核心局域网结构

双核心结构主要由两台三层交换机设备构建局域网核心。核心交换机与公共互联网相连。局域网内部的计算机结点通过接入交换机接入核心。

- 双核心结构局域网的主要特点：
  - ➢ 两台核心交换设备组成局域网核心，路由功能只存在于局域网核心；
  - ➢ 核心设备之间运行特定的网关保护或负载均衡协议，如 HSRP、VRRP、GLBP 等；
  - ➢ 网络结构可靠性高；
  - ➢ 设备投资比单核心高；
  - ➢ 网络覆盖范围较大，取决于核心设备之间互联的技术；
  - ➢ 可升级为层次局域网结构。

双核心典型结构如图 1-2 所示。

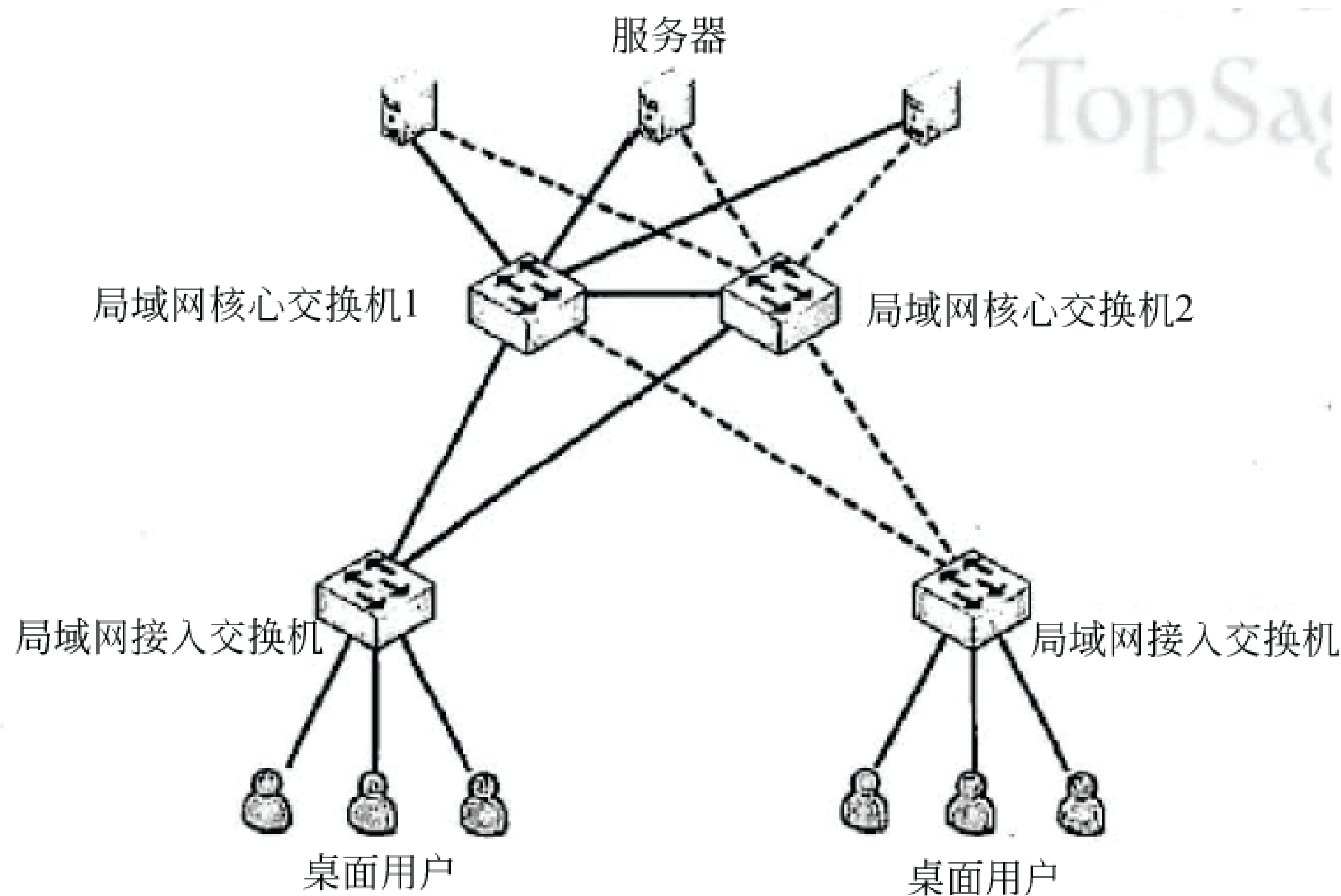


图 1-2 双核心局域网结构

- 环型局域网结构

环型局域网结构有多台核心三层设备连接成双 RPR 动态弹性分组环，构建整个局域网的核心。环型结构的局域网应用较少，其典型结构如下：

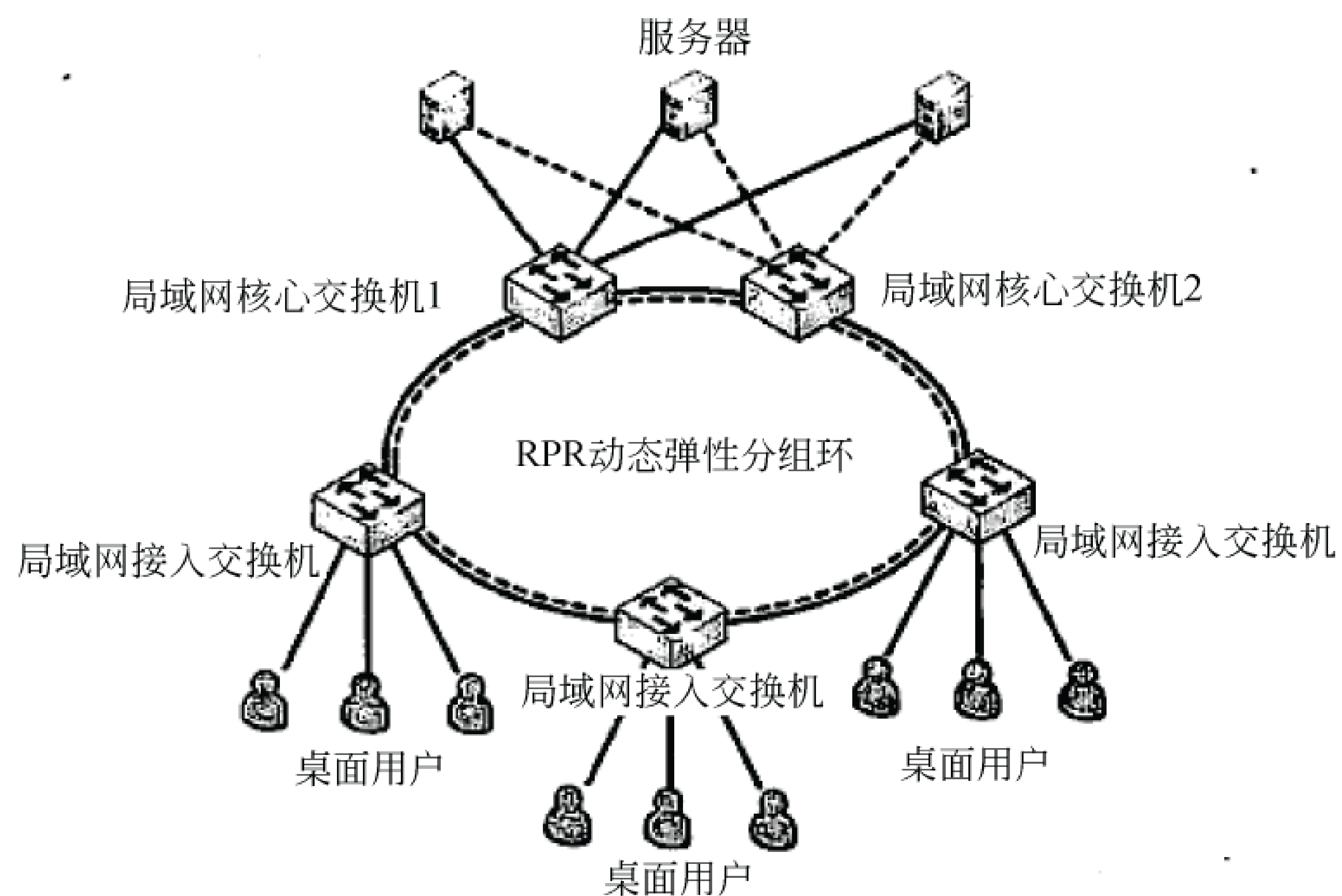


图 1-3　环型局域网结构

- 层次局域网结构

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定义为核心层、汇聚层、接入层。其典型结构如图 1-4 所示。

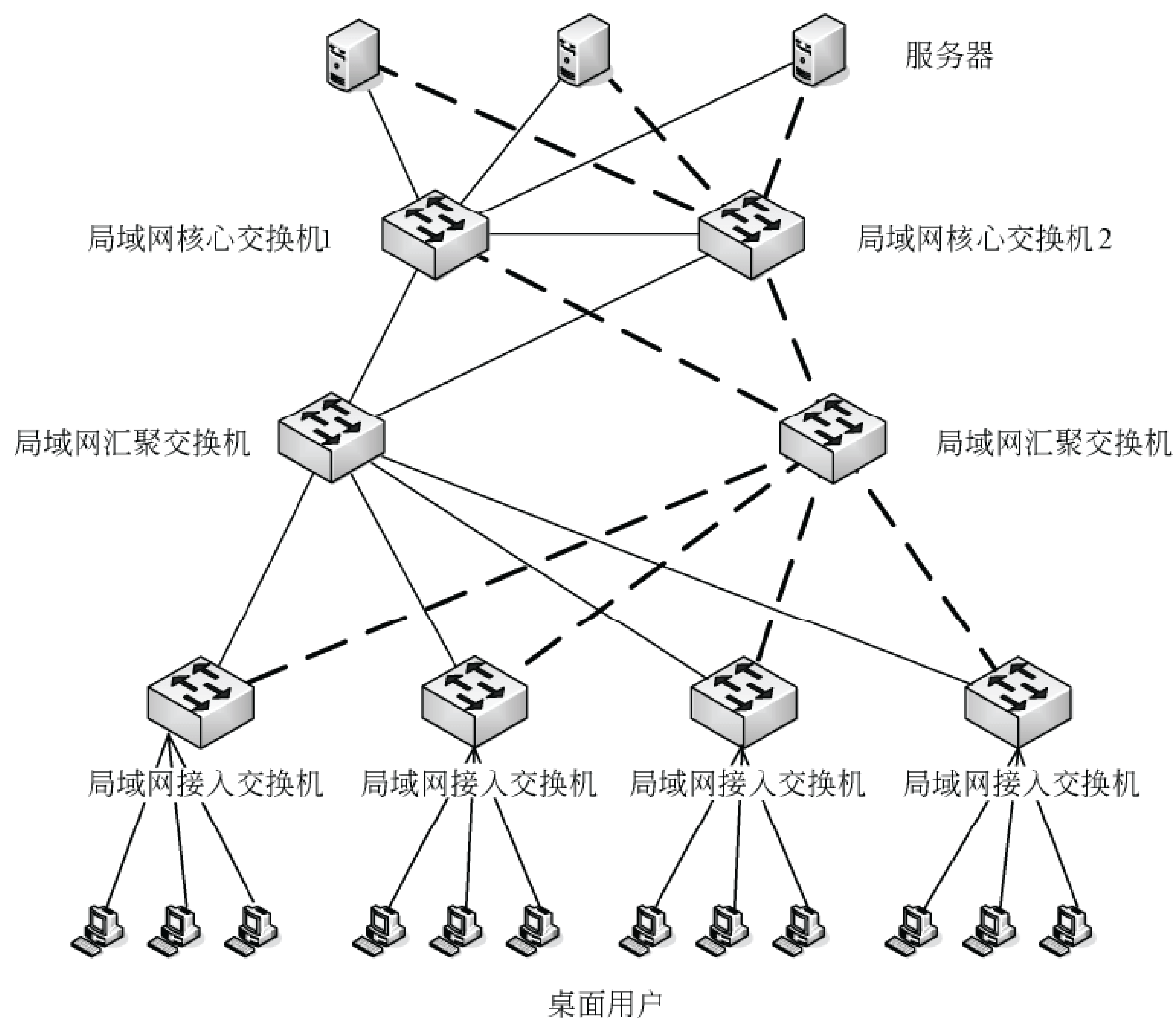


图 1-4　层次局域网结构

- 层次局域网主要特点：
  - 核心层实现高速数据转发；
  - 汇聚层实现丰富的接口和接入层之间进行互访控制；
  - 接入层实现用于接入；
  - 网络拓扑结构故障定位可分级便于维护；
  - 网络拓扑利用扩展；
  - 适用于大型的网络结构；
  - 网络投资大。

（4）广域网结构

典型的广域网结构有：单核心广域网结构、双核心广域网结构、环型广域网结构、半冗余广域网结构以及层次子域广域网结构。

广域网组网主要应用于大型的电信服务公司组网以及大型的跨国公司组网。

（5）局域网技术选择

目前可以使用的局域网技术有 IEEE 802 系列局域网技术、FDDI 技术和 ATM 技术，其中 IEEE 802 系列局域网技术主要有 IEEE 802.3。

从逻辑网络设计原则看，最佳的选择技术是 IEEE 802.3，即以太网技术。以太网技术的主要优势是：技术成熟；性价比高；组网、管理方便；支持多种速率和通信介质；支持除环型局域网以外的其他局域网结构。

（6）广域网技术选择

就企业网来说，主要考虑企业网如何接入 Internet，因此就本题的广域网技术选择来说，就是选择公共 Internet 的接入技术。

【问题 1】

从需求看，企业初期网络规模小，地理位置集中。可选择单核心结构的局域网结构。随着企业规模的扩大，可以升级为双核心结构或层次结构。从逻辑网设计原则看，局域网技术选择以太网技术。

以太网技术有：

- 10Mpbs 以太网技术

具体连网可选择 10Base-T 全双工、半双工交换式连接以及共享式连接。

- 100Mbp 以太网技术

100Base-TX 全双工、半双工交换式以及共享式连接。

100Base-FX 全双工、半双工交换式以及共享式连接。

- 1000Mbps 以太网技术

1000Mbps 以太网简称 GE，它是目前建设高速 LAN 的主要技术之一，其标准为 802.3z。千兆以太网标准出现之前，局域网主干采用 FDDI 或 ATM 技术。FDDI 是基于光纤的 100Mbps 局域网技术，是一个很成熟的技术，但价格相对较高。ATM 可以提供

从 155Mbps 以上的带宽，但技术复杂，设备价格高，维护管理复杂。100M 以太网技术用于组建骨干局域网，其性能和速率均显不足。千兆以太网的几种规范及应用领域如下表所示：

标准名称	节质类型	线缆直径	最大传输距离	主要应用领域
1000Base-SX	多模光纤	62.5 µm	260 m	适合大楼主干网
1000Base-SX	多模光纤	50 µm	525 m	适合大楼主干网
1000Base-LX	多模光纤	62.5 µm	550 m	适合大楼主干网
1000Base-LX	多模光纤	50 µm	550 m	适合大楼主干网
1000Base-LX	单模光纤	9 µm	3000 m	校园或城域网骨干
1000Base-T	5 类 UTP		100 m	适合大楼主干网
1000Base-CX	150Ω STP		25 m	集群网络设备互联

以太网连网主要设备有：交换机。

广域网接入技术分析如下：

单独考查 Internet，可以把接入 Internet 的技术分为两类：一类是传统的接入技术，一类是新兴的接入技术。

传统的接入技术有：

- 使用 Modem 经 PSTN 网络接入因特网。
- 专线接入。租用电信公司（NSP）的线路接入因特网。
- 局域网接入。由本地局域网直接接入因特网。
- 无线接入。通过无线网络接入因特网。

新兴的接入技术主要有：

- ADSL 技术。采用数字用户线技术通过电话线实现因特网接入。
- HDSL 技术。另一种采用数字用户线技术，通过电话线实现因特网接入。
- HFC 技术。通过 CATV 网络接入因特网。
- 光纤接入技术。以光纤为介质在用户和局端传输信息。

目前，针对企业用户，可以选择的接入技术主要是：ADSL 技术、专线技术、局域网接入和光纤接入。

ASDL 技术：上行速率最大 640Kbps，下行速率最大 8Mbps。主要特点：使用方便、投资少，适合主要为 Web 访问的网络；内部网络中不适合设置能对外提供公共服务的服务器。

专线接入：上下行速率相同。需要向电信部门（NSP）申请通信链路，通信链路一

般是由 FR 帧中继网络和 DDN 网络提供的。专线入网一般通过路由器把用户端和局端相连。专线入网有以下特点是：采用租用专线作为数据传输的通道；租用专线以包月制计费，费用较高；专线入网提供 64Kbps～100Mbps 的传输速率；适合小的集团用户。

局域网接入：本地局域网直接通过路由器与 Internet 相连。局域网接入的特点是：可以利用局域网本身的各种优点；可接入大量用户；通信速率高；可靠性高；费用适中；（平均分配到每个用户）；局域网本身自成体系，方便管理；适合大量的集群用户，如用户小区等。局域网接入需要一定的条件才能实现，即局域网和公共广域网设备在同一个地理位置。比如在一个校园内，校园本身是一个大型的局域网，而本校园又是 Internet 的一个区域结点，公共广域网设备就在校园内。

光纤接入：本地局域网通过光纤接入公共的 Internet。特点：通信速率高；扩展性好；可靠性高；费用最贵；适合对通信带宽、质量要求较高的用户选择。

总结：采用单核心交换式以太网；选择 10/100Mbps 自适应物理层；选择 ADSL 作为接入技术；50 人采用一个 C 类网（私有地址）即可，无需划分子网。

【问题 2】

本问题主要考查网络扩展问题。现在企业分为 4 个部分，对应 4 个局域网；从整体网络结构上看，可以选择的是：双核心局域网结构和层次局域网结构。针对企业整体网络结构，1000 人的企业应该属于中、大型企业，企业整体网络结构优先选择层次局域网结构（骨干层：双核心路由器，提供与公共 Internet 的双链路连接；汇聚层：分部的双核心路由器；接入层：分部的接入交换机）；企业分部（或总部）内的局域网，从可靠性要求上看，应选择双核心局域网结构（对应层次结构的汇聚层和接入层，汇聚层选择双核心）。

可靠性除考虑可靠的网络结构外，企业骨干层设备之间、局域网骨干设备之间以及骨干设备和局域网骨干设备之间应考虑采用 GE 光纤连接（单模光纤最远 3km，如使用新的光收发器，最远可达 70km，满足地理覆盖分布要求）。

分部和总部内的局域网接入交换机仍采用 10/100Mbps 自适应 5 类 UTP 连接。

Internet 接入技术可选择双 100Mbps 光纤局域网接入或 1000Mbp 光纤局域网接入。其他 100Mbps 以上、可靠的接入技术也可选择。（100Mbps 以太网接入，从综合效益上看是最佳选择）。

【问题 3】

问题 3 重点考查地址规划和信息隔离问题。

局域网上的信息隔离可以使用 VLAN 技术来解决；

子网划分总体需求是：

- 总体规模：

10000 人，至少每人一个 IP 地址；

其他地址：公共服务器地址；网络互联设备地址等。

考虑使用一个 B 类网。最多可容纳 65534 个 IP 地址。

- 总部+分部子网数：

50 个，每个包含 500 以上地址（可考虑 20%余量）

考虑：B 类网中增加 6bit 子网 ID：包含 64 个子网。每个子网最多可包含 1022 个 IP 地址。

- 总部或分部内部子网数：

10 个；最多 60 个地址

考虑：再增加 4bit 子网 ID，每个子网可再分为 16 个子网。每个子网最多可包含 62 个 IP 地址。

参考答案

【问题 1】

（1）因为网络规模较小，所以采用单核心局域网结构。配置一个核心二层或三层交换机，每个房间配备接入交换机。这种结构便于扩展和升级。

（2）物理层技术选择：通信介质选择 5 类 UTP 双绞线；网卡选择 10/100M 网卡。

（3）局域网技术选择：10/100/1000M 以太网技术。技术成熟，性价比最高，应用最广泛。

（4）广域网技术选择：由于初期无需对外提供互联网服务，入流量大于出流量，最佳接入技术是申请电信运营商的 ADSL 接入 Internet。

（5）地址规划：目前无需公网地址。采用私网地址即可。考虑初期人数最多 50 人，使用一个 C 类地址即可。如果每个房间需要隔离，可以使用 VLAN 并划分 IP 子网。

【问题 2】

（1）网络结构设计

总部局域网和分部局域网可以采用双核心局域网结构。

企业整体网络采用分层局域网结构，配备双核心路由器对外与互联网相连，对内与分部局域网的双核心交换机或路由器相连。

（2）物理层和局域网技术选择

总部局域网和分部局域网采用：10/100/1000M 以太网技术。通信介质可使用 5 类 UTP 双绞线或多模光纤。

总部局域网和分部局域网之间互联采用：1000BaseZX 以太网技术。通信介质：单模光纤。

（3）接入互联网技术选择

最佳方式：100Mbps 以太网接入。

其他可选方式：1000Mbps 以太网接入以及光纤接入（EPON）。

【问题 3】

（1）由于公司员工总数为 10000 人，考虑每人平均一个 IP 地址再加上公用设备地

址、服务器地址等公用地址，可使用一个 B 类网。可以选择 172.16.0.0/16～172.32.0.0/16 中的任意一个。

（2）首先需要对 B 类网划分 50 个以上的子网。这 50 个子网要满足两个条件：每个子网能包含 500 以上的可用 IP 地址，并且能继续划分为 10 个子网，再次划分的 10 个子网，每个子网要能包含 60 个可用的 IP 地址。

（3）举例

以 172.16.0.0/16 为例

采用/22 或 255.255.252.0 的子网掩码，可以把 B 类网划分为 64 个子网。（满足总部加分部 50 个）

172.16.0.0/22

172.16.4.0/22

…

172.16.252.0/22

每个子网再可划分 16 个子网：（满足每个总部或分部有 10 个部门）

以 172.16.4.0/22 为例：

172.16.4.0/26

172.16.4.64/26

每个子网可以包含最多 62 个 IP 地址（满足每个人一个 IP 地址）

试题二（30 分）

阅读下列说明，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

某单位的计算机网络结构如图 2-1 所示。

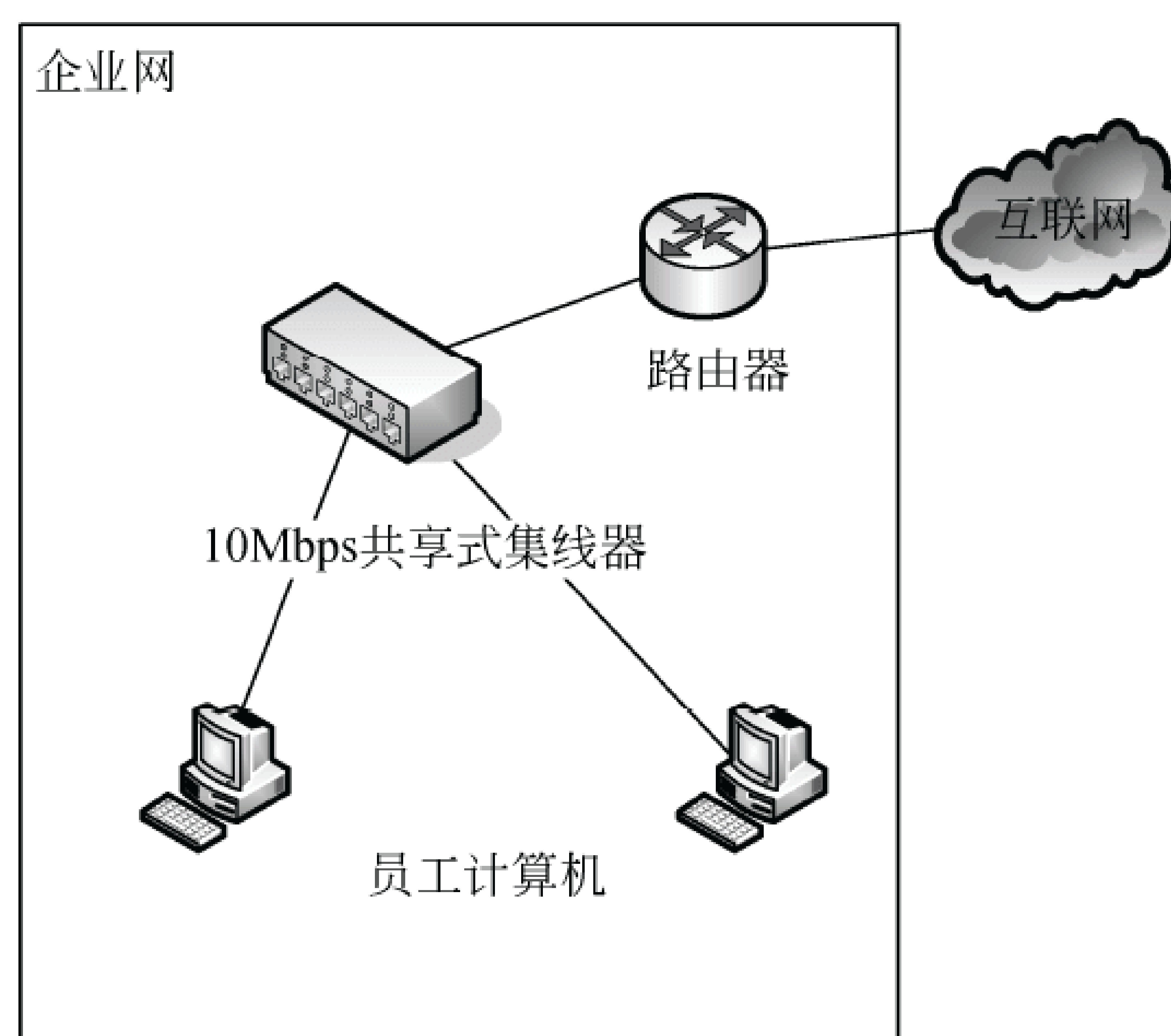


图 2-1　一个简单的初级网络

【问题 1】（5 分）

如果单位想把员工分组，每组的信息相互隔离，另外保证每个员工能独享 10Mbps 带宽，请指出：

最简单的升级方式是什么？对新设备的功能和性能有什么要求（接入的计算机数量不大于 20 个，要说明如何实现分组的信息隔离）。

【问题 2】（10 分）

随着单位规模的扩大，企业网络发展成了如图 2-2 所示的结构。公用服务器均位于主网段。主网段没有用户，均为公用设备。用户均匀分布在网段 1、网段 2 和网段 3。

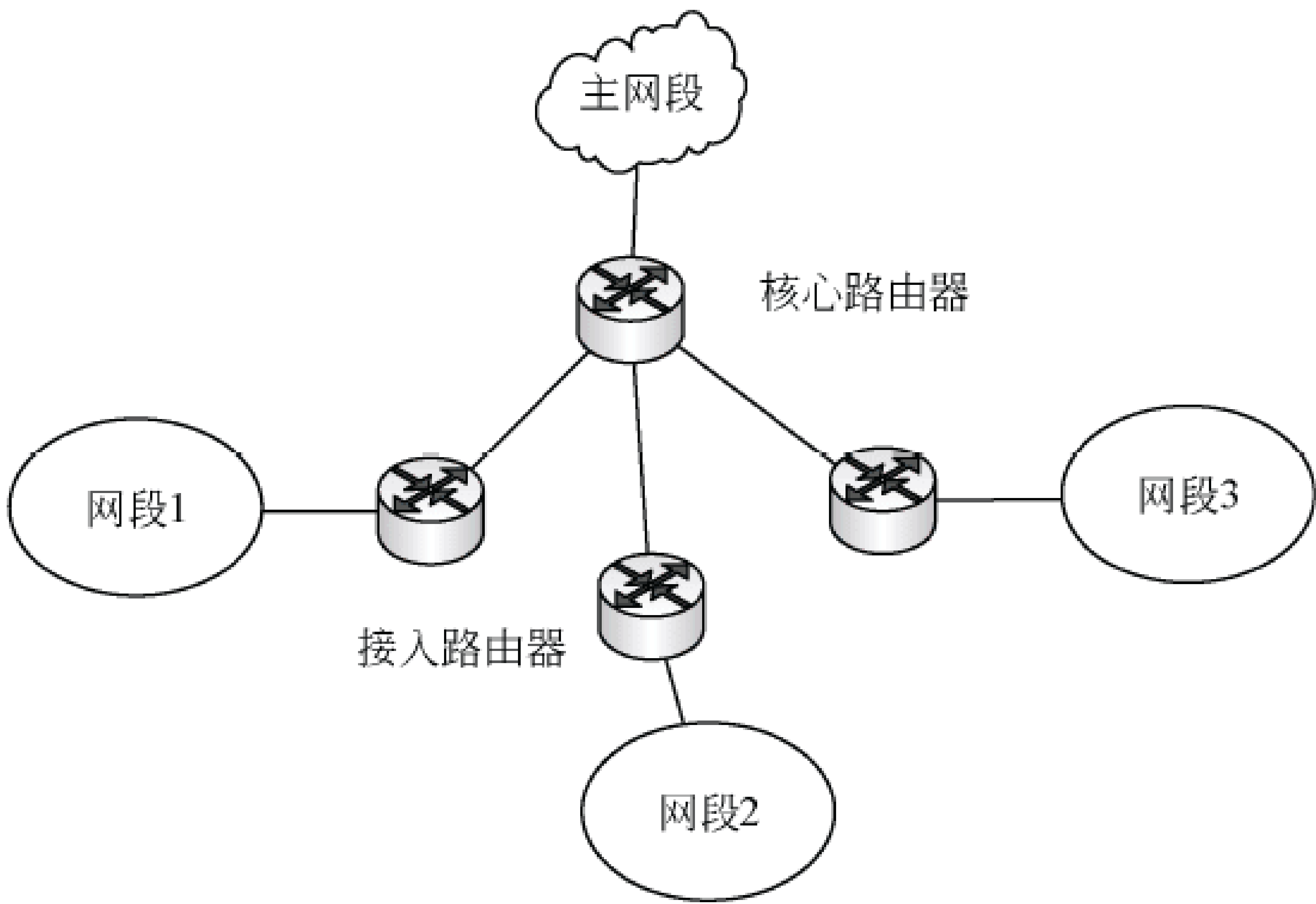


图 2-2　公司规模扩大后的网络结构

假定条件如下：

- 网段 1、2、3 大致相同，不考虑协议封装的开销。
- 用户收发邮件量大体相同。
- 内部交流属于用户之间的 P2P 流量，80%的流量发生在网段内部用户之间，20%的流量发生在不同网段的用户之间，且平均分配流量。
- 办公系统均为用户访问服务器，按上、下行不对称的一般原则分配流量。
- 视频监控流量按用户比例在不同网段之间平均分配，属于 P2P 流量。

请根据表 2-1 中已有的信息将出流量、入流量和网内流量填写完整；将表 2-2 的目的网段和总流量填写完整。

表 2-1　网段 2 用户流量分析表

业务种类	平均用户数	每用户平均流量	总流量	出流量	入流量	网内流量
邮件	150	0.32Mbps	48Mbps			
办公系统	300	0.16Mbps	48Mbps			
视频监控	20	2.4Mbps	48Mbps			
内部交流	600	0.008Mbps	4.8Mbps			

表 2-2 网段 2 的总流量分配表

流量分布	源网段	目的网段	总流量
网段内部	2		
访问服务器	2		
服务器反馈	主网段		
P2P	2		

【问题 3】（9 分）

（1）请计算出接入路由器内部交换流量、网段至主网段流量、网段之间流量和总流量。

（2）请计算出核心路由器的出、入流量和总流量。

（3）在 10/100/1000Mbps 的局域网技术中，应该选择哪一个作为网段内部互联技术（说明对路由器交换容量的最小要求）？

（4）在 10/100/1000Mbps 的局域网技术中，应该选择哪一个作为网段至主网段互联技术（说明对路由器交换容量的最小要求）？

（5）如果主网段和网段之间协议开销最大可增加 20%流量，是否需要升级网络？如果需要升级，最佳方案是什么？如果不需要升级，请说明原因。

【问题 4】（6 分）

参见本题图 2-2 。如果要提高普通网段访问主网段的可靠性和可用性，即在核心路由器出现故障时仍能访问主网段，请简要说明应该增加什么设备，新增设备与核心路由器之间可使用哪些协议以及这些协议之间主要有何区别。

试题二分析

试题二重点考查网络规划设计中的通信流量分析和依据流量对网络设备的选择。

【问题 1】

本问题主要考查对 VLAN、共享式以太网、交换式以太网的理解。

VLAN 可以把 LAN 划分成逻辑上信息隔离的区域；

共享式以太网连接时，连接在共享式集线器（HUB）上的所有计算机站点共享相同的带宽。

交互式以太网连接需要二层以太网交换机，每个端口连接一个计算机设备。交换式以太网可以实现独享带宽。VLAN 的划分必须是基于二层交换设备。集线器（HUB）不支持 VLAN 功能。

VLAN 的实现策略有很多种类，最简单的是基于二层交换机的物理端口划分 VLAN。其他 VLAN 划分策略还有：基于 MAC 地址；基于 IP 地址或协议等。

交换机性能计算原则：一个端口连接一台计算机。背板交换容量计算公式是：交换机的背板交换容量 =（交换机的端口数/2）× 每端口的标称速率 × 全双工系数。如果交换机支持全双工，则全双工系数为 2；如果只支持半双工，全双工系数为 1。

二层交换机的端口数量一般是 8、16、24、48。20 台计算机可选择 24 端口的交换机。

【问题 2】

（1）通信流量分布的简单规则

在通信规范分析中，最终的目标是产生通信量，其中必要的工作是分析网络中信息流量的分布问题。在整个过程中，需要依据需求分析的结果来产生单个信息流量的大小，依据通信模式、通信边界的分析，明确不同信息流在网络不同区域、边界的分布，从而获得区域、边界上的总信息流量。

对较为简单的网络，可以不需要进行复杂的通信流量分布分析，仅采用一些简单的方法，例如 80/20 规则、20/80 规则等；但是对于复杂的网络，仍必须进行复杂的通信流量分布分析。

（2）80/20 规则

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：在一个网段中，通信流量的 80%是在该网段内流动，只有 20%的通信流量是访问其他网段。

80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

（3）20/80 规则

随着互联网的发展，一些特殊的网络不断产生，例如小区内计算机用户形成的局域网、大型公司用于实现远程协同工作的工作组网络等。这些网络的特征就是：网段的内部用户之间相互访问较少，大多数网络访问都是对网段外的资源进行访问。对应这些流量分布则位于另一个极端，可以采用 20/80 规则。

20/80 规则的思路是：根据对用户和应用需求的统计，计算网段内的通信总量，其中 20%的通信流量是在该网段内流动，80%的通信流量是访问外部网段。

80/20 规则和 20/80 规则虽然比较简单，但这些规则是建立在大量的工程经验基础上的；另外通过这些规则的应用，可以很快完成一个复杂网络中大多数网段的通信流量分析工作，可以合理减少大型网络中的设计工作量。

（4）通信流量分析步骤

步骤一：把网络分成易管理的网段。

步骤二：确定个人用户和网段应用的通信流量。

步骤三：确定本地和远程网段上的通信流量。

步骤四：对每个网段重复步骤一、步骤二、步骤三。

步骤五：分析基于各网段信息的广域网和骨干网络的通信流量。

（5）常见互联网业务流量规则

E-mail：发送邮件和接收邮件（只与邮件服务器发生流量）。视为对等流量，即 50%流出，50%流入。

Web：浏览网络，从 Web 下载的流量大（只与 Web 服务器发生流量）。使用 20/80 法则。流出：20%，流入 80%。

FTP 或文件共享业务：等同电子邮件业务（只与 FTP 或文件共享服务器发生流量）。流入、流出各 50%。

办公自动化业务：等同 Web 业务（只与办公自动化服务器发生流量）。20%流出，80%流入。

视频监控：属于 P2P 业务类型（用户之间发生流量），在内部网络中流量平均分配。

内部交流：属于 P2P 业务类型（用户之间发生流量），80%发生在网段内部，20%发生在网段之间。

根据问题 2 给出的条件。网段 2 的流量计算如下：

电子邮件业务：总流量 48Mbps，50%流出本网段 24Mbps，50%流入本网段 24Mbps。无内部流量。

办公系统：总流量 48Mbps，20%流出本网段 9.6Mbps，80%流入本网段 38.4Mbps。无内部流量。

视频监控：总流量 48Mbps，三个网段平均分配，则外部流量占 2/3，即 32Mbps，流入流出各占 50%，即：流入 16Mbps、流出 16Mbps；网内流量占 1/3，即 16Mbps。

内部交流：总流量 4.8Mbps，20%网段之间流量，出入平均分配则流出：0.48Mbps、流入 0.48Mbps；80%网段内部，即 3.84Mbps。

【问题 3】

问题 3 依据问题 2 的流量分布进行计算。

按三个子网段相同来计算，以网段 2 为例。

接入路由器：

内部流量：视频监控内部流量 16Mbps+内部交流内部流量 3.84Mbps

网段至主网段流量（出流量+入流量）：48+48=96Mbps

网段之间的流量（出流量+入流量）：32+0.96=32.96Mbps

总流量：48*3+4.8 = 148.8Mbps

核心路由器：

网段之间转发流量（出流量+入流量）：32.96Mbps*3 = 98.88Mbps

网段到主网段流量（出流量+入流量）：96Mbps*3 = 288Mbps

总流量：286.88Mbps

路由器背板交换容量选择原则：大于总流量，并有 20%～30%的冗余。取整为 200Mbps 的整数倍。

【问题 4】

本问题主要考查单核心局域网结构和双核心局域网结构在可靠性方面的区别，以及双核心局域网结构中核心设备之间重要的可靠性协议（冗余备份协议、流量均衡协议）。

单核心局域网结构的主要缺点是，核心结点故障将导致整个网络瘫痪（不可用），增加可靠性和可用性的最佳方法是增加一台新的核心路由器。两台核心路由器之间运行 VRRP 协议、HSRP 协议或 GLBP 协议。

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种容错协议。通常，一个网络内的所有主机都设置一条缺省路由，这样，当主机发出数据包的目的地址不在本网段时，报文将被通过缺省路由发往网关路由器，从而实现了主机与外部网络的通信。当某网络的默认网关（路由器）故障时，本网段内所有主机将不能与外部网络通信。VRRP 就是为解决这一严重问题而提出的，它为具有多播或广播能力的局域网设计。VRRP 将局域网的一组路由器（包括一个 Master 即主控路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器，称之为一个备份组。

在 VRRP 协议中，有两组重要的概念：VRRP 路由器和虚拟路由器，主控路由器和备份路由器。VRRP 路由器是指运行 VRRP 的路由器，是物理实体，虚拟路由器是指 VRRP 协议创建的，是逻辑概念。一组 VRRP 路由器协同工作，共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色：主控路由器和备份路由器，一个 VRRP 组中有且只有一台处于主控角色的路由器，可以有一个或者多个处于备份角色的路由器。VRRP 协议使用选择策略从路由器组中选出一台作为主控路由器，负责 ARP 响应和转发 IP 数据包，组中的其他路由器作为备份的角色处于待命状态。当主控路由器发生故障时，其中一台备份路由器能在几秒钟的时延后升级为主路由器。由于切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对用户是透明的。

HSRP 是 Cisco 开发的热备份路由协议，与 VRRP 基本功能类似。GLBP 协议与 VRRP 和 HSRP 功能类似，但能够实现负载均衡功能。

参考答案

【问题 1】

（1）用二层交换机取代 10M 共享式集线器。

（2）二层交换机需要支持 VLAN 功能，通过 VLAN 的划分，不同的 VLAN 对应不同的员工组，VLAN 之间的信息相互隔离。

（3）VLAN 策略可以通过基于交换机物理端口的策略来划分。接入不同端口的员工加入不同的 VLAN，即加入了不同的组。

（4）对交换机性能方面，可以使用 24 端口的 10/100Mbps 自适应以太网交换机。

（5）背板交换容量最低应达到 10×24 / 2 = 120Mbps。如果考虑所有端口 100Mbps 速率，则背板交换容量最低应达到 1.2Gbps。

【问题 2】

网段 2 用户流量分析表。

业务种类	出流量	入流量	网内流量
邮件	24Mbps	24Mbps	无
办公系统	9.6Mbps	38.4Mbps	无
视频监控	16Mbps	16Mbps	16Mbps
内部交流	0.48Mbps	0.48Mbps	3.84Mbps

网段 2 的总流量分配表。

流量分布	目的网段	总流量
网段内部	2	19.84Mbps
访问服务器	主网段	33.6Mbps
服务器反馈	2	62.4Mbps
P2P	网段 1 或网段 3	32.96Mbps

【问题 3】

（1）接入路由器：

网段内部交换流量：19.84Mbps

网段至主网段流量：48Mbps+48Mbps=96Mbps

网段之间流量：32.96Mbps

总流量：48×3 + 4.8 = 148.8Mbps

（2）核心路由器：

网段与主网段之间总流量：96Mbps×3 = 288Mbps

其中：主网段到网段流量（出流量）：（24+38.4）×3 = 187.2Mbps

网段到主网段流量（入流量）：（24+9.6）×3 = 100.8Mbps

网段之间的转发流量：32.96Mbps×3 = 98.88Mbps

总流量：286.88Mbps

（3）网段内部选择 100Mbps 以太网技术，接入路由器背板交换容量在 200Mbps 以上。

（4）网段和主网段之间选择 100Mbps 以太网技术交互式连接，核心路由器背板交换容量在 400Mbps 以上。

（5）需要升级网络。核心路由器和接入路由器之间采用全双工 100Mbps 交换式连接。核心路由器背板交换容量 600Mbps 以上。

【问题 4】

（1）再增加一个核心路由器。

（2）两个核心路由器之间运行 VRRP、HSRP 协议或 GLBP 协议。

VRRP 协议是公开的虚拟路由器冗余协议。HSRP 是 Cisco 开发的热备份路由协议。

（3）VRRP 和 HSRP 基本功能类似，其缺点是存在路由器闲置问题。GLBP 协议与 VRRP 和 HSRP 功能类似，但能够实现负载均衡功能。

试题三（15 分）

阅读以下关于某机构网络的叙述，回答问题 1、问题 2 和问题 3。

某机构打算新建一个网络，其中有内部办公计算机若干台，内部数据库服务一台，内部文件传输（FTP）服务器一台，网页（Web）服务器一台，邮件服务器一台。要求能对外提供万维网（WWW）访问和邮件服务，内部办公计算机和内部数据库、文件传输（FTP）服务器对外不可见。

【问题 1】（6 分）

请划分该机构网络的安全区域和安全级别，说明各机器属于哪个区域和级别。

【问题 2】（6 分）

为提高安全性，请设计该机构网络的防火墙方案，画出拓扑图，并给出防火墙的相关规则的配置策略。

【问题 3】（3 分）

如果想要监听、检测内部办公计算机之间的连接和攻击，应该在何位置配置何种设备？画出相关拓扑图。

试题三分析

本题涉及网络安全区域的划分、防火墙和入侵检测等的内容。

【问题 1】

要保障一个网络系统的安全，首先应该分析该网络系统的特点和安全需求，分析对外需要提供的服务，评估需要保护的数据的安全级别和面临的风险，划分不同的安全区域，然后再制定系统安全策略，决定实现时采用何种方式和手段。

本题所述机构的网络中有内部数据库服务和内部文件传输（FTP）服务器各一台，内部办公计算机若干台。服务器上存储的数据信息量大，且是内部数据，安全级别要求最高，内部办公计算机处理的数据也是内部数据，不对外公开，其安全级别也可定位最高。因此这些机器应该统一划分在同一个安全区域，以便采用统一的安全策略来实施重点保护。

本题所述机构的网络中有网页（Web）服务器和邮件服务器各一台。由于要求能对外提供万维网（WWW）访问服务和邮件服务，则这两台服务器对本机构网络外部的设备是可见的，外部设备会访问这两台服务器，可能会受到外网不安全因素的威胁，其安全级别会降低。因此不能同内部服务器等放在同一区域，以免在遭受攻击时影响内部网络。因此这两台服务器应该统一划分在同一个安全区域，以便采用统一的安全策略来统一实施保护，以保证能对外提供正常的服务。

本机构网络之外的因特网设备和主机，能访问该机构网络中有网页（Web）服务器和邮件服务器，这部分设备和主机是不可信的、要防备的区域，安全级别最低，可划分为同一个安全区域。

【问题 2】

防火墙的典型体系结构（部署方式）有三种形式：双重宿主主机体系结构、屏蔽主机体系结构、屏蔽子网体系结构，具体部署时需根据网络的特点和具体的安全需求、安全策略来决定。

防火墙的双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络和内部网络的任务。一个典型的双宿主主机防火墙如图 3-1 所示，它使用一个双宿主主机完成防火墙功能。该主机至少有两个网络接口，一个是内部网络接口，一个是因特网接口，故称为双宿主主机。

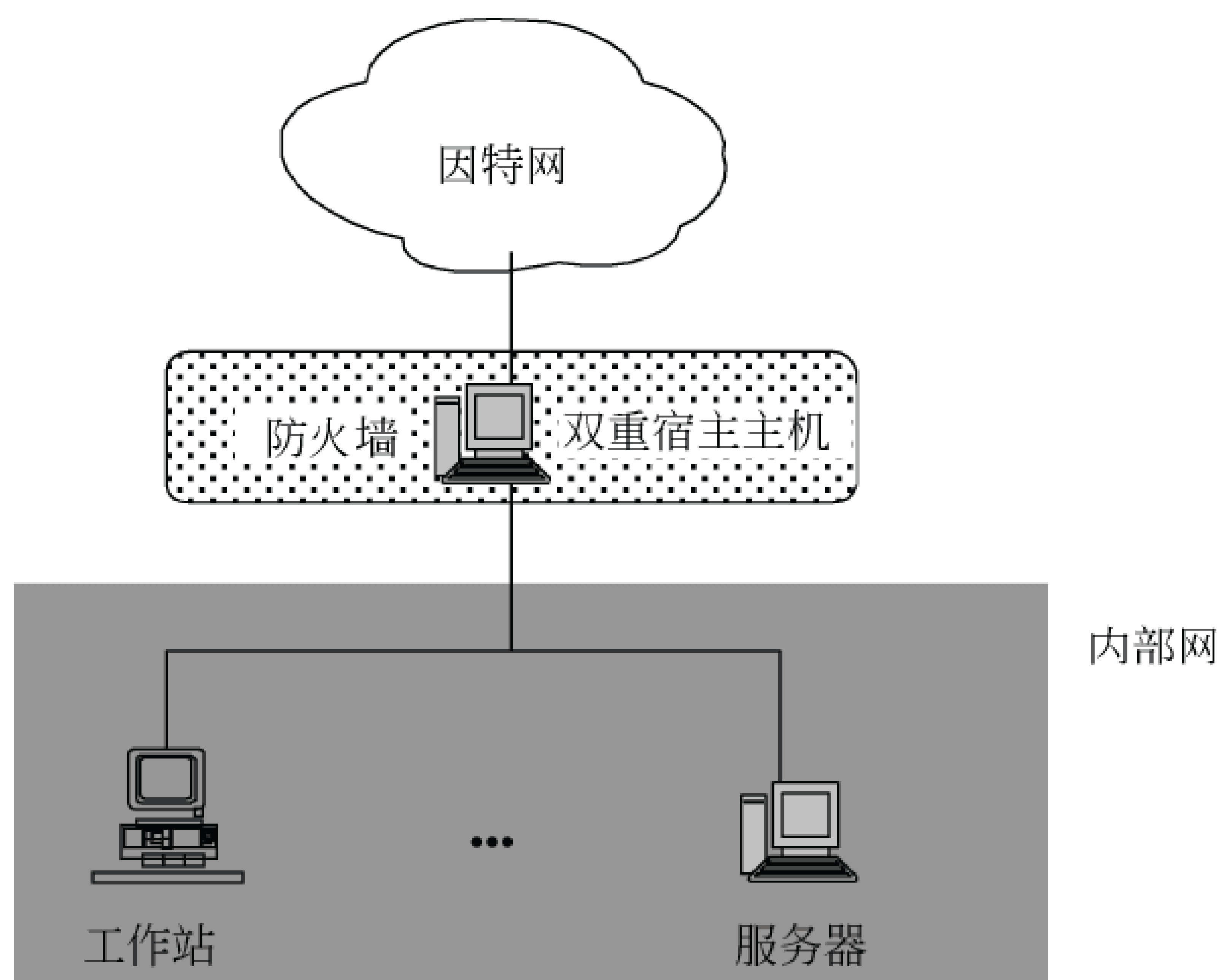


图 3-1　双宿主主机结构防火墙

防火墙的屏蔽主机体系结构如图 3-2 所示，通过屏蔽路由器和堡垒主机结合的方式来构造防火墙。其中屏蔽路由器是一个单独的路由器，采用包过滤方式来实现内、外部网络的隔离和对内网的保护，而堡垒主机是因特网中的主机能够访问的唯一的内部网中的主机，内部网中的其他主机对外都是不可见的，故称为屏蔽主机防火墙。

堡垒主机通常是安全管理员标识的作为网络安全中关键点的系统，这类系统健壮安全，能抗攻击，故称为堡垒主机。在屏蔽主机防火墙中，堡垒主机用于对外提供一定的服务，如 WWW 服务，而且任何外部的主机只有通过这台主机才能得到内部系统的服务（在外部主机看来，没有内部网络，只有堡垒主机）。由于堡垒主机暴露在因特网中，故堡垒主机需保持较高的安全等级，具有一定的抗攻击能力。

防火墙的屏蔽子网体系结构的最简单形式如图 3-3 所示，防火墙由外部屏蔽路由器、内部屏蔽路由器和堡垒主机共同组成。与前两种防火墙体系结构有明显区别的是，在外/内部屏蔽路由器间有一个称为非军事化区的子网，进一步将内部网络同因特网隔离开来，起到屏蔽内部网络的作用，提供更进一步的安全性，故称为屏蔽子网防火墙。

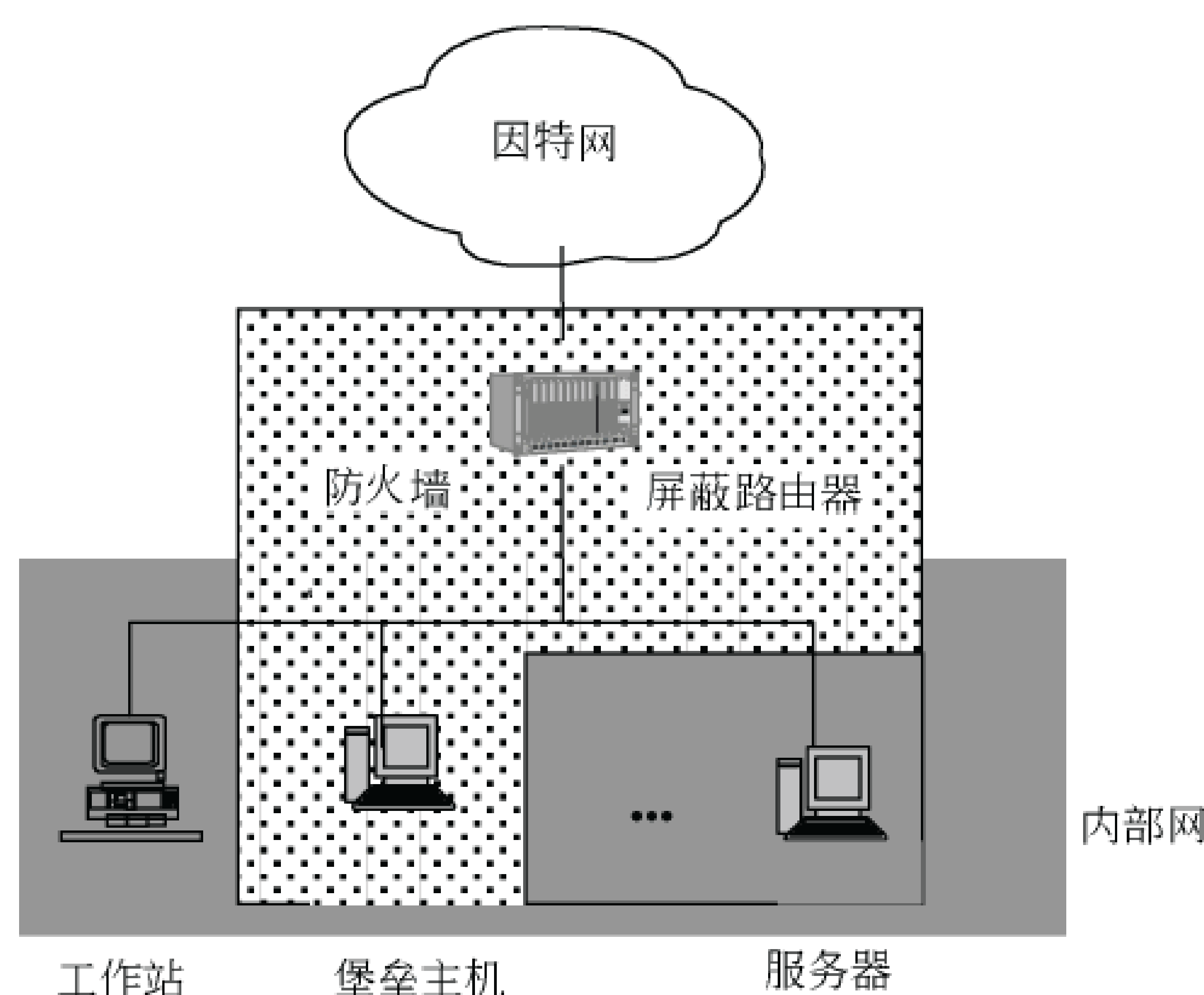


图 3-2　屏蔽主机体系结构防火墙

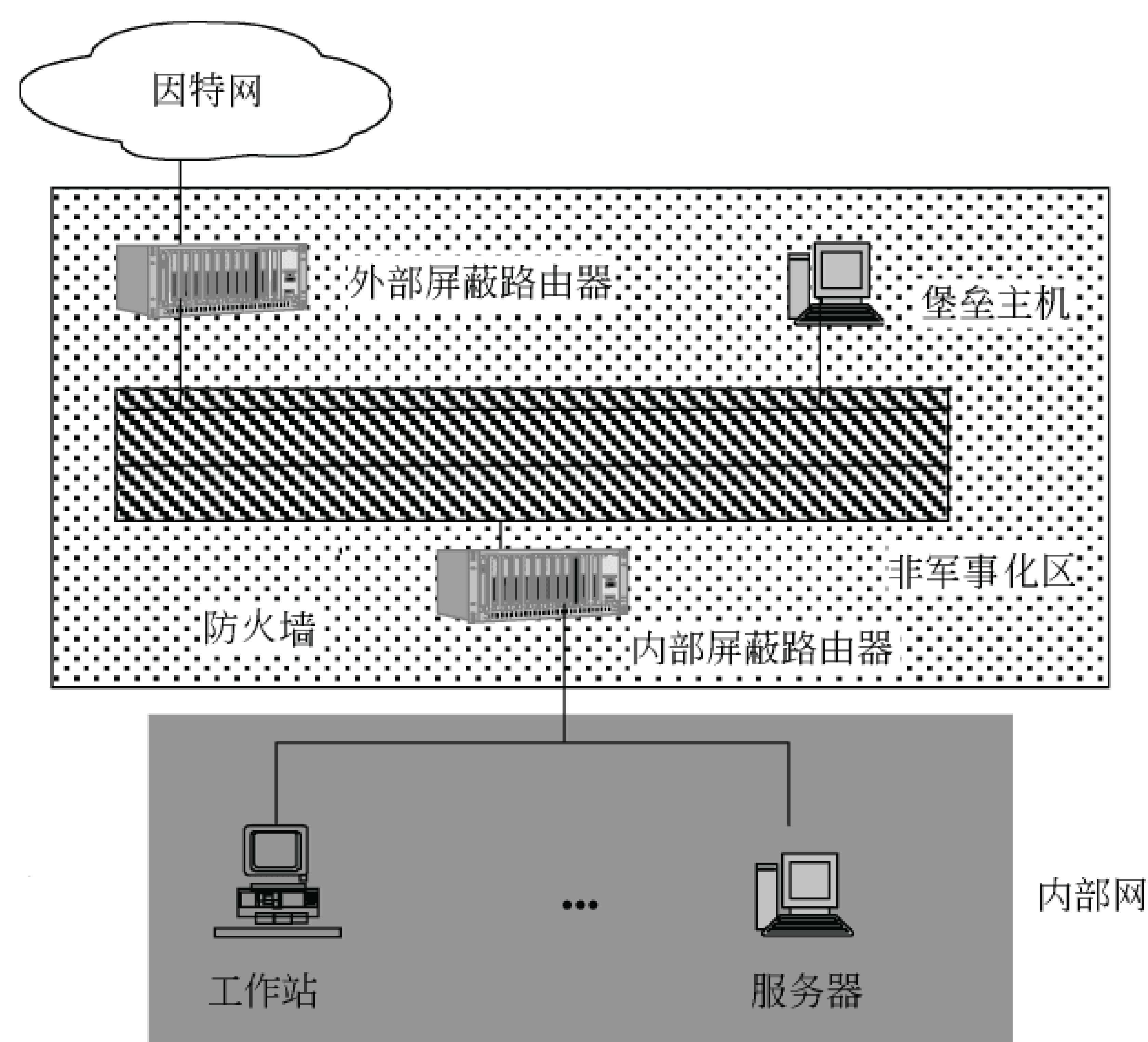


图 3-3　屏蔽子网结构防火墙

非军事化区即 DMZ：De-Militarized Zone，原指古代战场上交战双方的开火区及后方保护区之间的隔离地带，在该隔离地带中，会有一些冲突和一定的危险，但危害性不大且容易控制，而且在大规模战争爆发前能及时告警。此概念用于网络安全中是指额外的安全保护子网，信任度较低、易受攻击的对外提供服务的服务器和堡垒主机都放置在该子网中，远离内部网络。DMZ 概念的出现源于用户对防火墙使用中的需求，早期简单的防火墙提供的是内部网与外部网之间的边界保护，而内部网中对外提供服务的服务器（如邮件服务器）比其他的内部网的机器遭到入侵的可能性要高很多，且这些服务器一旦被入侵，将被用来作为跳板攻击整个内部网。有了非军事化区后，一旦入侵者侵入非军

事化区，最坏会损坏其中的服务器和堡垒主机，但不会损伤到内部网的完整性，而且通过在周边网络上隔离对外提供服务的服务器和堡垒主机，还减少了网络安全对堡垒主机的依赖。非军事化区中的主机主要通过主机安全来保证其安全性。

屏蔽子网防火墙使用了两个屏蔽路由器，消除了内部网络的单一侵入点，增强了网络的安全性。但两个屏蔽路由器的规则设置的侧重点不同。

配置防火墙的访问策略时，一般按服务来配置规则。首先要分析网络的特点及网络对外提供的服务，弄清各服务的工作原理及正常的工作流程，然后再分析各服务在防火墙环境下如何工作，并对服务配置。

【问题 3】

防火墙和操作系统加固技术等传统安全技术都是静态安全防御技术，不能提供足够的安全性；入侵检测系统能使系统对入侵事件和过程做出实时响应，提供系统的动态安全性。

入侵检测系统是通过从计算机网络和系统的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定措施的技术。

入侵检测系统包括三部分内容：信息收集、信息分析和响应。其中收集信息的可靠性和正确性在很大程度上决定了入侵检测系统的有效性和准确性。需要在合适的位置上放置，以保证采集信息的准确性和充足性。

参考答案

【问题 1】

整个网络分为三个不同级别的安全区域：

1．内部网络：安全级别最高，是可信的、重点保护的区域。包括所有内部办公计算机，内部数据库服务器和内部 FTP 服务器。

2．外部网络：安全级别最低，是不可信的、要防备的区域。包括外部因特网用户主机和设备。

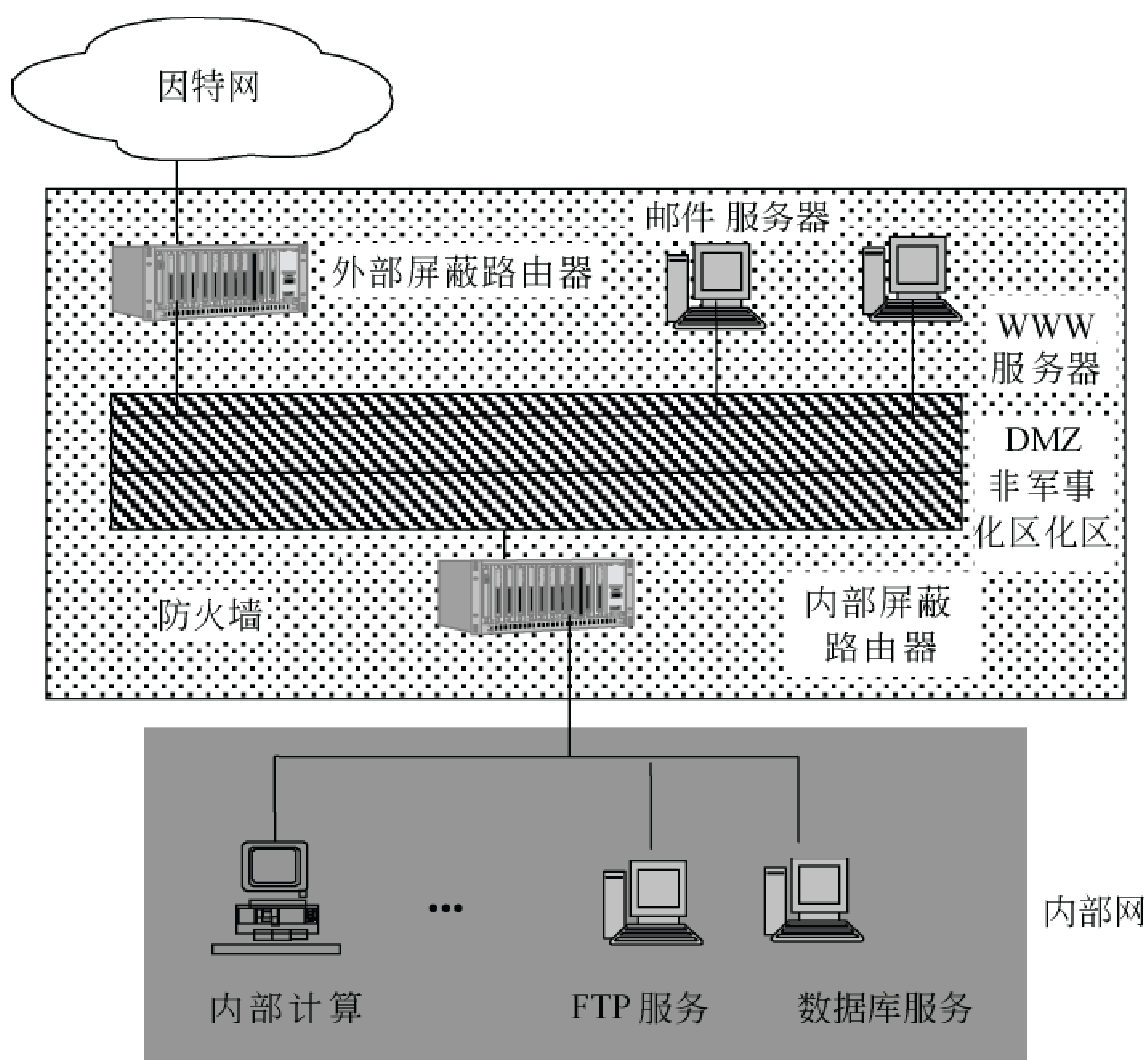
3．DMZ 区域（非军事化区）：安全级别中等，因为需要对外开放某些特定的服务和应用，受一定的保护，是安全级别较低的区域。包括对外提供 WWW 访问的 Web 服务器和邮件服务器。

【问题 2】

配置策略：

外部屏蔽路由区的访问策略：允许外部网络客户访问 DMZ 区的 WWW 服务器提供的 WWW 服务和邮件服务器提供的邮件服务，其他禁止；

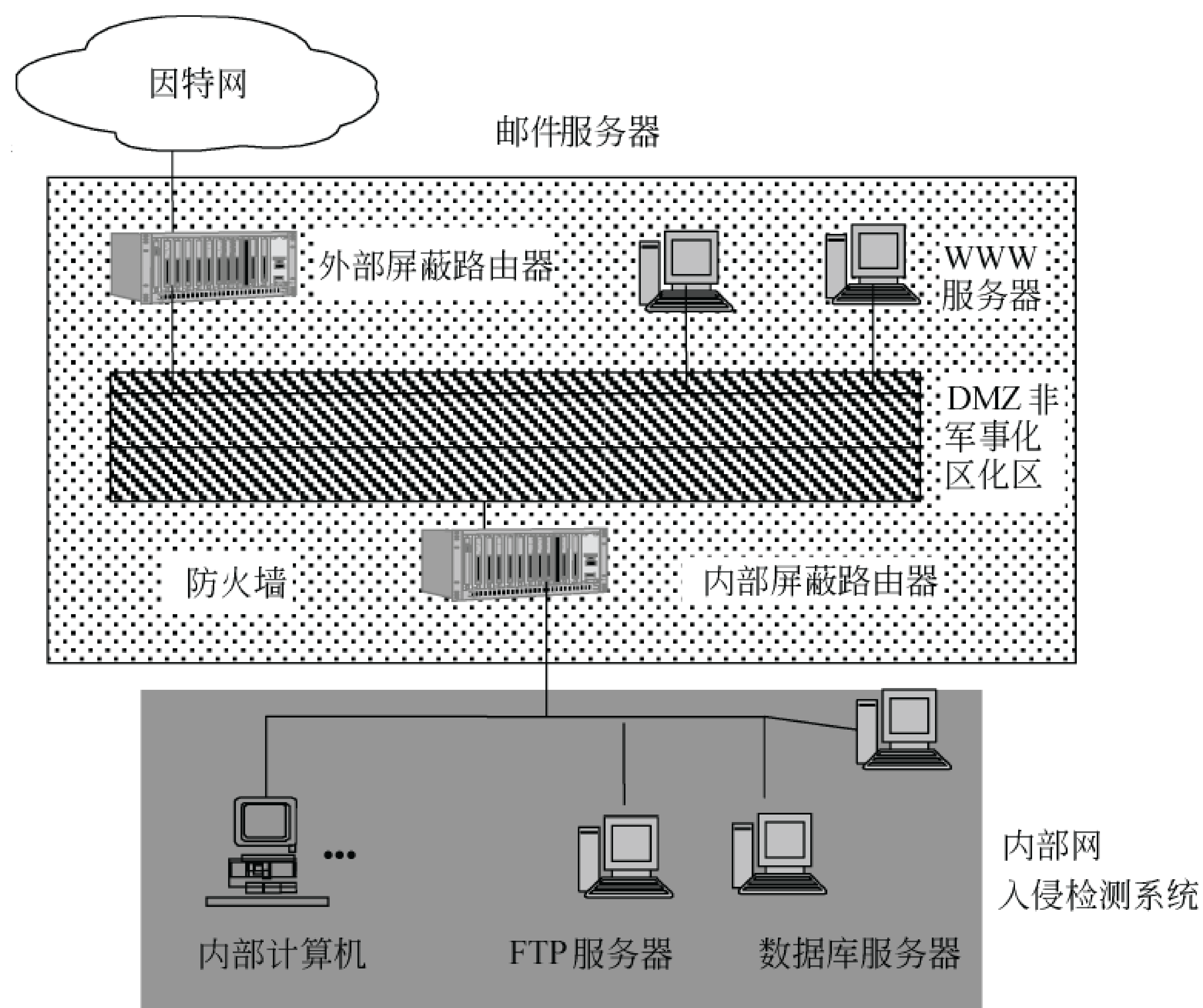
内部屏蔽路由器的访问策略：允许内部网客户访问外部网络，不允许外部网络客户访问内部网；允许内部网客户访问 DMZ 区，不允许 DMZ 区网络客户访问内部网。



【问题 3】

（1）应该配置入侵检测系统（IDS 系统）。

（2）拓扑图为：



第12章　2011下半年网络规划设计师下午试卷II写作要点

试题一　论计算机网络系统设计中接入技术的选择

计算机网络技术的发展非常迅速，新技术不断涌现。在网络设计和实现中，各种接入方式和接入技术不断成熟，要求在网络规划和设计中，考虑实际情况，针对具体目标，选择适合的接入方式和技术。

请围绕“计算机网络系统设计中接入技术的选择”论题，依次对以下三个方面进行论述。

1．简要叙述你参与设计和实施的计算机网络项目，以及你所担任的主要工作和接入方式的选择。

2．详细论述你在网络规划和设计中接入技术选择的思路与策略，以及所采用的技术和方法。

3．分析和评估你所采用的接入技术的措施及其效果，以及相关的改进措施。

写作要点

1．叙述自己参与设计和实施的计算机网络项目，该项目应有一定的规模，自己在该项目中担任的主要工作应有一定的份量，说明自己对接入技术的选择。

2．从使用场景来考虑：

接入技术主要有局域网接入，宽带无线接入，远程接入和光网络接入技术等几种。

局域网接入是最常采用的接入方式，用户计算机的网卡通过双绞线连到以太网交换机，以太网交换机之间通过光纤、同轴电缆、双绞线等组网或接入到其他计算机网络，双绞线总长度一般不超过100米，线路距离短，因而线路质量得到了更好的保障。接入带宽一般比较高，可以达到10Mbps～1000Mbps，稳定可靠，价格比较低。

宽带无线接入技术主要使用WIFI技术，WIFI基于IEEE 802.11系列标准，工作在2.4G频段，可以达到54Mbps带宽，覆盖范围达到100m，增强天线可以达到5Km左右，成本下降很快，应用很广泛，但由于采用无线传输，有安全问题。

计算机远程接入计算机网络，可以采用PSTN接入、ISDN接入、CABLE接入、数字用户环路DSL接入。PSTN接入是将计算机通过Modem连接到电话线上，通过电话网将计算机和计算机网络连接起来，计算机网络中添加远程访问服务器，传输速率较低，最高只有56kbps；ISDN接入是计算机利用ISDN网络提供的两种接口（基本速率接口和基群速率接口）完成计算机网络的接入，基本速率接口带宽最多128Kbps，基群速率接口可达2Mbps。数字用户线路（Digital Subscriber Line DSL）接入技术在传统的电话

线上提供高速的数据传输服务，ADSL 的应用最广，已经成为城域网接入的主要技术，ADSL 的上下行流量不对称，有 1.544～9Mbps 的高速下行信道、有 16～640Kbps 的上行信道、64Kbps 的语音信道，三个信道可以同时工作。ADSL 接入需要的设备包括接入设备（局端设备 DSLAM 和用户端设备 ATU-R），用户线路和管理服务器。

光纤接入分为有源和无源两类。有源接入基于 SDH 的多业务传送平台（MSTP）、基于以太网或 ATM 的多业务接入平台等。然而，这种技术作为有源设备仍然无法完全摆脱电磁干扰和雷电影响，以及有源设备固有的维护问题。无源光网络（PON）是一种很有吸引力的纯介质网络，其主要特点是避免了有源设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，提高了系统可靠性，同时节省了维护成本，PON 由于具有简洁、廉价、可靠的网络拓扑结构，被普遍认为是宽带接入网的最终解决方案，分为 APON、EPON、GPON。

3．对选择的网络系统设计中接入技术的效果以及需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

试题二　论计算机网络系统的可靠性设计

计算机网络规划和设计的可靠性问题是一个关键问题，是网络规划和设计所必须考虑的，其目的是提高网络系统的可靠性，保证网络系统的稳定运行。

请围绕“计算机网络系统的可靠性设计”论题，依次对以下三个方面进行论述。

1．简要叙述你参与的计算机网络项目和你所承担的主要工作，以及项目的可靠性要求。

2．从接入、网络、设备和系统等方面，讨论网络设计的可靠性的解决方案和措施。

3．评估在网络设计中你采用可靠性的措施所带来的好处和问题。

写作要点

1．叙述自己参与设计和实施的计算机网络项目，自己在该项目中承担的主要工作，网络项目所采用的可靠性措施。

2．计算机网络设计要采用可靠性技术，骨干设备要考虑到容错和冗余，即当某一个模块或设备出现故障，是否影响其他模块或设备正常工作，是否支持热插拔，是否支持备份设备的自动切换，当网络设置多个相同设备，是否支持负荷分担，或出现问题时能否自动切换。

物理层不稳定，必然导致承载的应用出现故障，应尽量选择较为稳定、可靠的物理层技术。在实现远程用户的接入时，不选择基于模拟信号调制的语音拨号接入方式，而是选择基于数字信号编码的 ISDN 或者 ADSL 方式。例如，在专网建设中，如果用户存在变动或升级带宽的需求，则不能采用带宽固定的 SDH 信道，而是采用可以动态变化带宽的 ATM PVC 方式。

无线局域网络同样可以实现冗余，提供了 AP 的热备份功能。

局域网交换机之间设计冗余链路，冗余链路存在着备份和负载分担两种应用方式。

交换机作为局域网的核心设备，其可靠性保障有链路聚合、冗余网关、以太网供电、多业务模块等。采用链路聚合后，可靠性大大提高，因为多条链路中只要有一条可以正常工作，则这个链路就可以工作。除此之外，链路聚合可以实现负载均衡和负载分担。网络至少提供两台交换机成为各个 VLAN 的网关，避免网关的单点故障，常用的冗余网关协议有 VRPP、HSRP 和 GLBP。

为了提高服务器的性能、工作负载能力和可靠性，一般设置几台服务器。常采用的技术有负载服务均衡器、网络地址转换、使用 DNS 解析及双机热备的高可用技术等。

系统可采用集群技术，独立磁盘冗余阵列技术等。

3．在网络设计中采用可靠性措施所带来的好处和问题，比如成本、管理和维护等。

第 13 章　2012 下半年网络规划设计师上午试题分析与解答

试题（1）、（2）

假设系统中有 n 个进程共享 3 台打印机，任一进程在任一时刻最多只能使用 1 台打印机。若用 PV 操作控制 n 个进程使用打印机，则相应信号量 S 的取值范围为__（1）__；若信号量 S 的值为-3，则系统中有__（2）__个进程等待使用打印机。

（1）A. 0，-1，…，-(n-1)　　B. 3，2，1，0，-1，…，-(n-3)
　　C. 1，0，-1，…，-(n-1)　　D. 2，1，0，-1，…，-(n-2)

（2）A. 0　　B. 1　　C. 2　　D. 3

试题（1）、（2）分析

本题考查操作系统进程管理方面的基础知识。

根据题意假设系统中有 n 个进程共享 3 台打印机，意味着每次只允许 3 个进程进入互斥段，那么信号量的初值应为 3。可见，根据排除法只有选项 B 中含有 3。

信号量 S 的物理意义为：当 S≥0 时，表示资源的可用数；当 S<0 时，其绝对值表示等待资源的进程数。

参考答案

（1）B　（2）D

试题（3）、（4）

CRM 是一套先进的管理思想及技术手段，它通过将__（3）__进行有效的整合，最终为企业涉及到的各个领域提供了集成环境。CRM 系统的四个主要模块包括__（4）__。

（3）A. 员工资源、客户资源与管理技术
　　B. 销售资源、信息资源与商业智能
　　C. 销售管理、市场管理与服务管理
　　D. 人力资源、业务流程与专业技术

（4）A. 电子商务支持、呼叫中心、移动设备支持、数据分析
　　B. 信息分析、网络应用支持、客户信息仓库、工作流集成
　　C. 销售自动化、营销自动化、客户服务与支持、商业智能
　　D. 销售管理、市场管理、服务管理、现场服务管理

试题（3）、（4）分析

本题考查企业信息化的基本知识。

CRM 是一套先进的管理思想及技术手段，它通过将人力资源、业务流程与专业技术进行有效的整合，最终为企业涉及到客户或者消费者的各个领域提供了完美的集成，

使得企业可以更低成本、更高效率地满足客户的需求，并与客户建立起基于学习性关系基础上的一对一营销模式，从而让企业可以最大程度提高客户满意度和忠诚度。CRM 系统的主要模块包括销售自动化、营销自动化、客户服务与支持、商业智能。

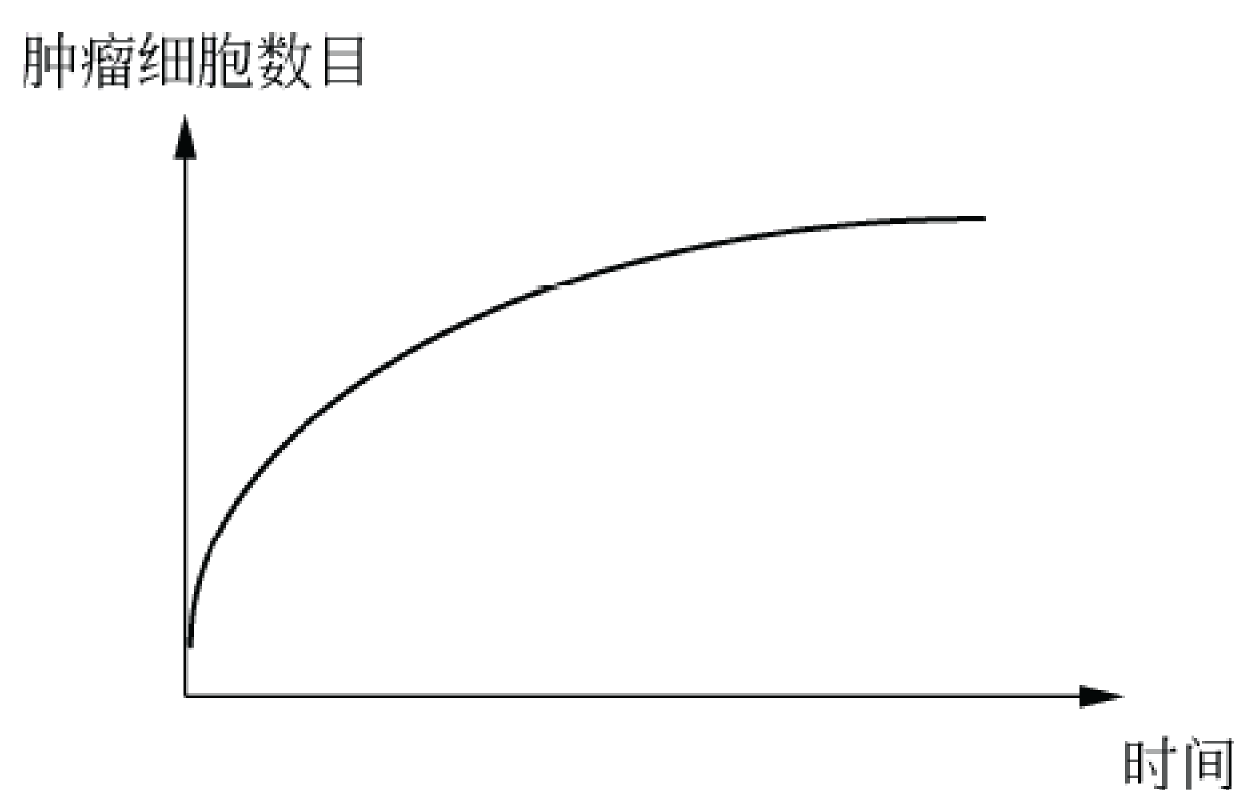
参考答案

（3）D （4）C

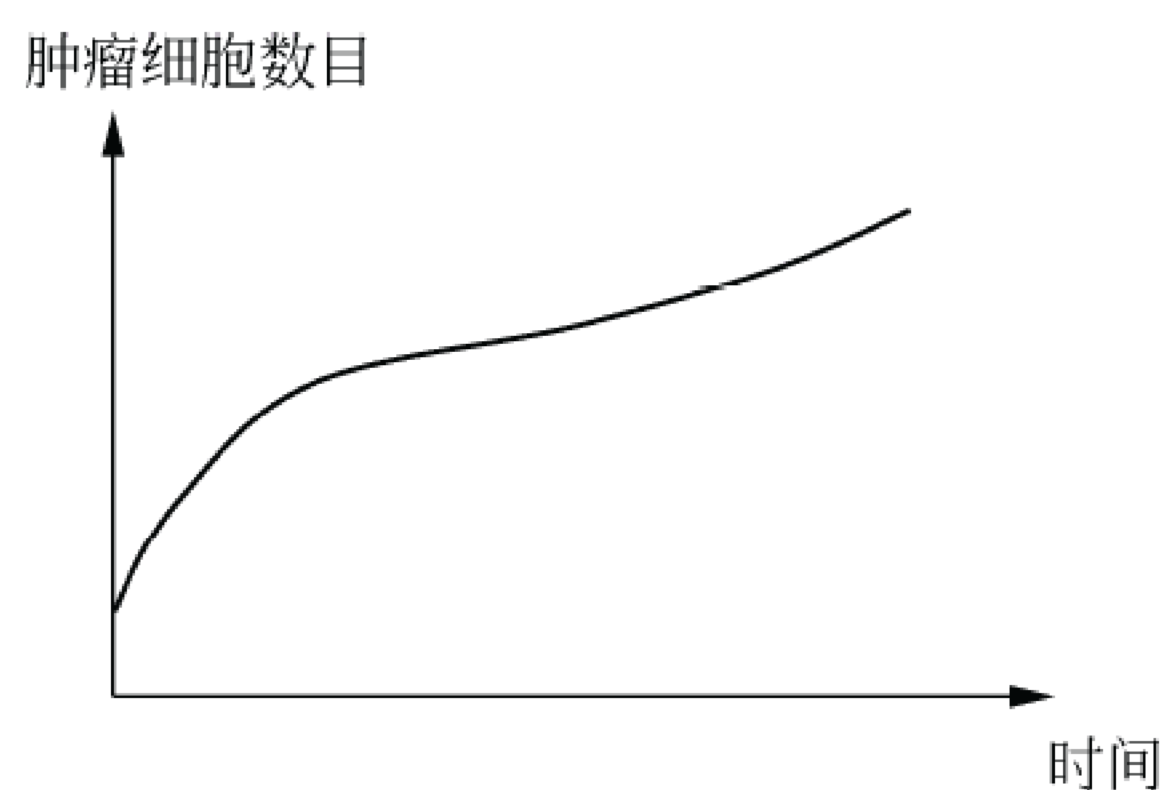
试题（5）

研究表明，肿瘤的生长有以下规律：当肿瘤细胞数目超过 10^{11} 时才是临床可观察的；在肿瘤生长初期，几乎每隔一定时间就会观测到肿瘤细胞数量翻一番；在肿瘤生长后期，肿瘤细胞的数目趋向某个稳定值。为此，图__（5）__反映了肿瘤的生长趋势。

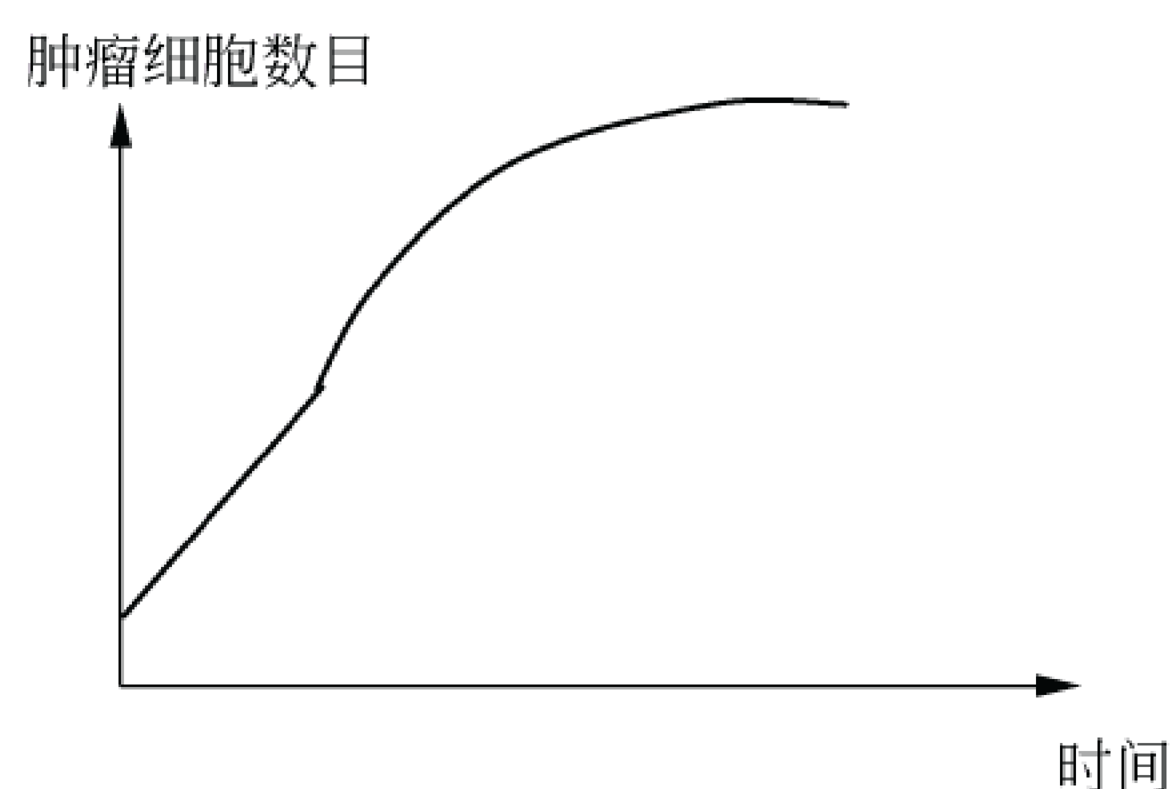
（5）A.



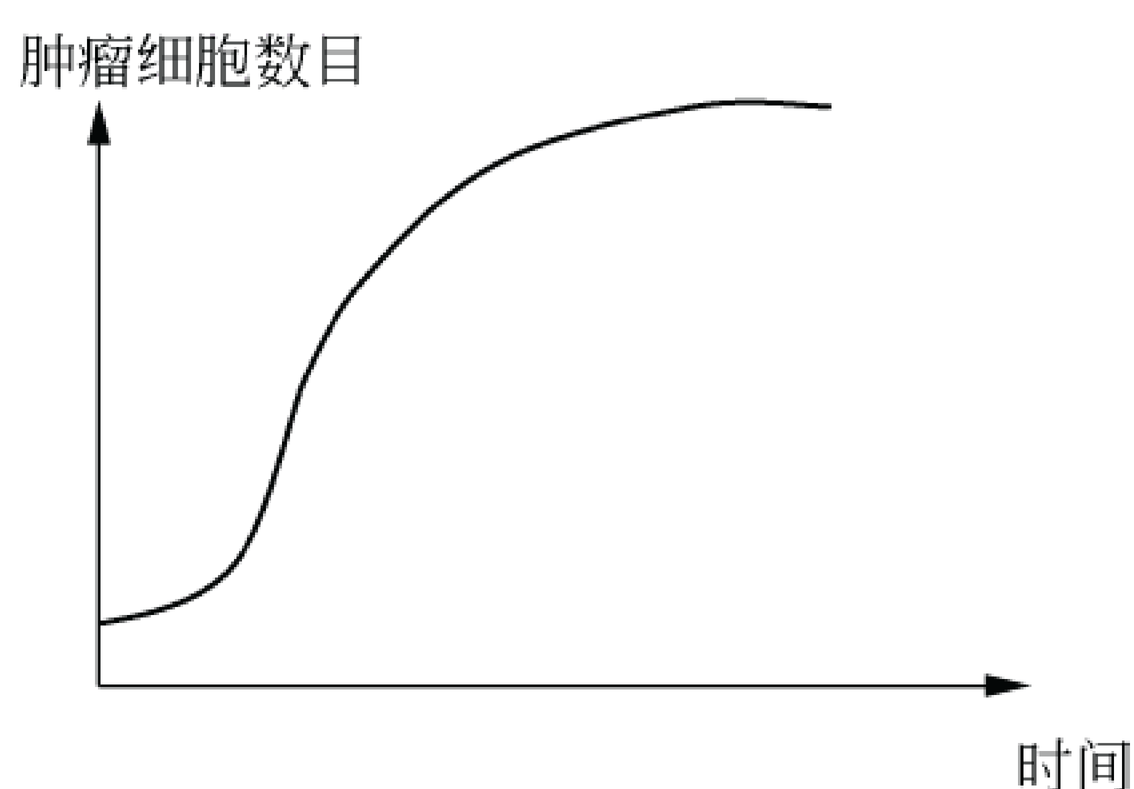
B.



C.



D.



试题（5）分析

本题考查应用数学基础知识。

用函数曲线来表示事物随时间变化的规律十分常见。可以用函数 f(t)表示肿瘤细胞数量随时间变化的函数。那么，当肿瘤细胞数目超过 10^{11} 时才是临床可观察的，可以表示为 $f(0)= 10^{11}$。在肿瘤生长初期，几乎每隔一定时间就会观测到肿瘤细胞数量翻一番，可以表示为 $t<t_0$ 时，$f(t+c)=2f(t)$。符合这种规律的函数是指数函数：$f(t)=a^t$，其曲线段呈凹形上升态。在肿瘤生长后期，肿瘤细胞的数目趋向某个稳定值，表示当 t>T 时，f(t) 逐渐逼近某个常数，即函数曲线从下往上逐渐靠近直线 y=L。

参考答案

（5）D

试题（6）

九个项目 A11，A12，A13，A21，A22，A23，A31，A32，A33 的成本从 1 百万，2 百万，……，到 9 百万各不相同，但并不顺序对应。已知 A11 与 A21、A12 与 A22 的成本都有一倍关系，A11 与 A12、A21 与 A31、A22 与 A23、A23 与 A33 的成本都相差 1 百万。由此可以推断，项目 A22 的成本是__（6）__百万。

（6）A．2　　B．4　　C．6　　D．8

试题（6）分析

本题考查应用数学基础知识。

为便于直观分析，题中的叙述可以用下图来表示：

A11	A12	A13
A21	A22	A23
A31	A32	A33

九个项目 A_{ij}（i=1，2，3；j=1，2，3）的成本值（单位为百万，从 1 到 9 各不相同）将分别填入 i 行 j 列对应的格中。格间的黑点表示相邻格有一倍关系，白点表示相邻格相差 1。

已知 A22 与 A12 的值有一倍关系，那就只可能是 1-2，2-4，3-6 或 4-8，因此 A22 的值只可能是 1，2，3，4，6，8。

如果 A22=1，则 A23=A12=2，出现相同值，不符合题意。

如果 A22=2，则 A12 只能是 4（A12=1 将导致 A11=A22=2 矛盾），A23 只能为 3（A23=1 将导致 A33=A22=2 矛盾），A33 出现矛盾。

如果 A22=3，则 A12=6，A11=5 或 7，不可能与 A21 有一倍关系。

如果 A22=4，则 A12=2 或 8。A12=8 将导致 A11=7 或 9，不可能与 A21 有成倍关系。因此 A12=2，A23 只能是 5（A23=3 将导致 A33 矛盾），A33=6，而 A11=1 或 3 都将导致 A21 矛盾。

如果 A22=8，则 A12=4，A23 只能是 7（A23=9 将导致 A33=8 矛盾），A33 只能是 6，A11 只能是 3（A11=5 将导致 A21 矛盾），A21=6 矛盾。

因此，A22 只可能为 6。

实际上，当 A22=6 时，A12=3，A23 只能为 7（A23=5 将最终导致矛盾），A33=8。此时，A11、A21、A31 可能分别是 2、4、5，也可能是 4、2、1。

参考答案

（6）C

试题（7）

以下关于软件生存周期模型的叙述，正确的是__（7）__。

（7）A．在瀑布模型中，前一个阶段的错误和疏漏会隐蔽地带到后一个阶段

B．在任何情况下使用演化模型，都能在一定周期内由原型演化到最终产品

C．软件生存周期模型的主要目标是为了加快软件开发的速度

D．当一个软件系统的生存周期结束之后，它就进入到一个新的生存周期模型

试题（7）分析

软件产品从形成概念开始，经过开发、使用和维护，直到最后退役的全过程成为软件生存周期。一个完整的软件生存周期是以需求为出发点，从提出软件开发计划的那一刻开始，直到软件在实际应用中完全报废为止。软件生存周期的提出是为了更好地管理、维护和升级软件，其中更大的意义在于管理软件开发的步骤和方法。

软件生存周期模型又称软件开发模型（software develop model）或软件过程模型（software process model），它是从某个特定角度提出的软件过程的简化描述。软件生存周期模型主要有瀑布模型、演化模型、原型模型、螺旋模型喷泉模型和基于可重用构件的模型等。

瀑布模型是最早使用的软件生存周期模型之一。瀑布模型的特点是因果关系紧密相连，前一个阶段工作的结果是后一个阶段工作的输入。或者说，每一个阶段都是建立在前一个阶段的正确结果之上，前一个阶段的错误和疏漏会隐蔽地带入后一个阶段。这种错误有时甚至可能是灾难性的，因此每一个阶段工作完成后，都要进行审查和确认。

演化模型主要针对事先不能完整定义需求的软件开发，是在快速开发一个原型的基础上，根据用户在调用原型的过程中提出的反馈意见和建议，对原型进行改进，获得原型的新版本，重复这一过程，直到演化成最终的软件产品。演化模型的主要优点是，任何功能一经开发就能进入测试，以便验证是否符合产品需求，可以帮助引导出高质量的产品要求。其主要缺点是，如果不控制地让用户接触开发中尚未稳定的功能，可能对开发人员及永固都会产生负面的影响。

参考答案

（7）A

试题（8）

以下关于软件测试工具的叙述，错误的是__（8）__。

（8）A．静态测试工具可用于对软件需求、结构设计、详细设计和代码进行评审、走查和审查

B．静态测试工具可对软件的复杂度分析、数据流分析、控制流分析和接口分析提供支持

C．动态测试工具可用于软件的覆盖分析和性能分析

D．动态测试工具不支持软件的仿真测试和变异测试

试题（8）分析

测试工具根据工作原理不同可分为静态测试工具和动态测试工具。其中静态测试工具是对代码进行语法扫描，找到不符合编码规范的地方，根据某种质量模型评价代码的质量，生成系统的调用关系图等。它直接对代码进行分析，不需要运行代码，也不需要对代码编译链接和生成可执行文件，静态测试工具可用于对软件需求、结构设计、详细设计和代码进行评审、走审和审查，也可用于对软件的复杂度分析、数据流分析、控制流分析和接口分析提供支持；动态测试工具与静态测试工具不同，它需要运行被测试系统，并设置探针，向代码生成的可执行文件中插入检测代码，可用于软件的覆盖分析和性能分析，也可用于软件的模拟、建模、仿真测试和变异测试等。

参考答案

（8）D

试题（9）

企业信息化程度是国家信息化建设的基础和关键，企业信息化方法不包括＿（9）＿。

（9）A．业务流程重组　　B．组织机构变革

C．供应链管理　　D．人力资本投资

试题（9）分析

本题考查企业信息化的基本方法。

企业信息化程度是国家信息化建设的基础和关键，企业信息化就是企业利用现代信息技术，通过信息资源的深入开发和广泛利用，实现企业生产过程的自动化、管理方式的网络化、决策支持的智能化和商务运营的电子化，不断提高生产、经营、管理、决策的效率和水平，进而提高企业经济效益和企业竞争力的过程。企业信息化方法主要包括业务流程重构、核心业务应用、信息系统建设、主题数据库、资源管理和人力资本投资方法。企业战略规划是指依据企业外部环境和自身条件的状况及其变化来制定和实施战略，并根据对实施过程与结果的评价和反馈来调整，制定新战略的过程。

参考答案

（9）B

试题（10）

中国 M 公司与美国 L 公司分别在各自生产的平板电脑产品上使用 iPad 商标，且分别享有各自国家批准的商标专用权。中国 Y 手电筒经销商，在其经销的手电筒高端产品上也使用 iPad 商标，并取得了注册商标。以下说法正确的是＿（10）＿。

（10）A．L 公司未经 M 公司许可在中国市场销售其产品不属于侵权行为

B．L 公司在中国市场销售其产品需要取得 M 公司和 Y 经销商的许可

C．L 公司在中国市场销售其产品需要向 M 公司支付注册商标许可使用费

D．Y 经销商在其经销的手电筒高端产品上使用 iPad 商标属于侵权行为

试题（10）分析

本题考查知识产权知识，涉及商标权的相关概念。知识产权具有地域性的特征，按照一国法律获得承认和保护的知识产权，只能在该国发生法律效力，即知识产权受地域限制，只有在一定地域内知识产权才具有独占性（专用性）。或者说，各国依照其本国法律授予的知识产权，只能在其本国领域内受其国家的法律保护，而其他国家对这种权利没有保护的义务，任何人均可在自己的国家内自由使用外国人的知识产品，既无须取得权利人的许可，也不必向权利人支付报酬。

通过缔结有关知识产权的国际公约的形式，某一国家的国民（自然人或法人）的知识产权在其他国家也能取得权益。参加知识产权国际公约的国家，会相互给予成员国国民的知识产权保护。虽然众多知识产权国际条约等的订立，使地域性有时会变得模糊，但地域性的特征不但是知识产权最“古老”的特征，也是最基本的特征之一。目前知识产权的地域性仍然存在，如是否授予权利、如何保护权利，仍须由各成员国按照其国内法来决定。依据我国商标法五十二条规定，未注册商标不得与他人在同一种或类似商品上已经注册的商标相同或近似。若未经商标注册人的许可，在同一种商品或者类似商品上使用与他人注册商标相同或者近似的商标的，属于侵犯专用权的行为，应当承担相应的法律责任。

知识产权的利用（行使）有多种方式，许可使用是其之一，它是指知识产权人将自己的权利以一定的方式，在一定的地域和期限内许可他人利用，并由此获得报酬（即向被许可人收取一定数额的使用费）的法律行为。对于注册商标许可而言是指注册商标所有人通过订立许可使用合同，许可他人使用其注册商标的法律行为。

依据我国商标法规定，不同类别商品（产品）是可以使用相同或类似商标的，如在水泥产品和化肥产品都可以使用“秦岭”商标，因为水泥产品和化肥产品是不同类别的产品。但对于驰名商标来说，不能在任何商品（产品），使用与驰名商标相同或类似的标识。

参考答案

（10）C

试题（11）

在下面 4 个协议中，属于 ISO OSI/RM 标准第二层的是__（11）__。

（11）A．LAPB　　B．MHS　　C．X.21　　D．X.25 PLP

试题（11）分析

LAPB 是 X.25 公用数据网中的数据链路层协议，实际上是 HDLC 的子集，采用了异步平衡通信方式。MHS 是 CCITT 在 X.400 标准中定义的报文处理系统（Message Handling System），它是一种在广域网平台上运行的电子邮件系统。X.21 是一种物理层接口标准，终端设备通过这种接口连接公用数据网。X.25 PLP 是公用数据网中的分组层

协议，通过虚电路为数据终端提供面向连接的服务。

参考答案

（11）A

试题（12）

下面有关无连接通信的描述中，正确的是__（12）__。

（12）A．在无连接的通信中，目标地址信息必须加入到每个发送的分组中

B．在租用线路和线路交换网络中，不能传送 UDP 数据报

C．采用预先建立的专用通道传送，在通信期间不必进行任何有关连接的操作

D．由于对每个分组都要分别建立和释放连接，所以不适合大量数据的传送

试题（12）分析

计算机网络为用户提供面向连接的服务和无连接的服务。面向连接的服务需要三个阶段：建立连接，数据传送和释放连接。无连接的服务没有建立连接和释放连接的开销，而是把目标地址直接加入到传送的报文中，通过逐段路由，最后转发到达目标。在 TCP/IP 网络中，TCP 协议提供端到端的面向连接的数据传送服务，UDP 提供端到端的无连接服务，IP 协议在网络层提供无连接的数据报服务。在传输层和网络层提供什么类型的服务与底层协议和网络的基础设施没有关系。在逻辑上说，下层可以提供任何类型的服务，而上层则通过自己的功能实现面向连接或无连接的通信。所以在租用专线或线路交换网络中都可以实现 UDP 数据报的传送。

参考答案

（12）A

试题（13）

在 PPP 链路建立以后，接着要进行认证过程。首先由认证服务器发送一个质询报文，终端计算该报文的 Hash 值并把结果返回服务器，然后服务器把收到的 Hash 值与自己计算的 Hash 值进行比较以确定认证是否通过。在下面的协议中，采用这种认证方式的是__（13）__。

（13）A．CHAP　　B．ARP　　C．PAP　　D．PPTP

试题（13）分析

PPP 扩展认证协议可支持多种认证机制，并且允许使用后端服务器来实现复杂的认证过程，例如通过 Radius 服务器进行 Web 认证时，远程访问服务器（RAS）只是作为认证服务器的代理传递请求和应答报文，并且当识别出认证成功/失败标志后结束认证过程。通常 PPP 支持的两个认证协议是：

口令验证协议（Password Authentication Protocol，PAP）：提供了一种简单的两次握手认证方法，由终端发送用户标识和口令字，等待服务器的应答，如果认证不成功，则终止连接。这种方法不安全，因为采用文本方式发送密码，可能会被第三方窃取；

质询握手认证协议（Challenge Handshake Authentication Protocol，CHAP）：采用三

次握手方式周期地验证对方的身份。首先是逻辑链路建立后认证服务器就要发送一个挑战报文（随机数），终端计算该报文的 Hash 值并把结果返回服务器，然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较，如果匹配，则认证通过，连接得以建立，否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与，而密钥是不通过网络传送的，所以 CHAP 是更安全的认证机制。在后续的通信过程中，每经过一个随机的间隔，这个认证过程都可能被重复，以缩短入侵者进行持续攻击的时间。值得注意的是，这种方法可以进行双向身份认证，终端也可以向服务器进行挑战，使得双方都能确认对方身份的合法性。

参考答案

（13）A

试题（14）

下面有关 ITU-T X.25 建议的描述中，正确的是__（14）__。

（14）A. 通过时分多路技术，帧内的每个时槽都预先分配给了各个终端

B. X.25 的网络层采用无连接的协议

C. X.25 网络采用 LAPD 协议进行数据链路控制

D. 如果出现帧丢失故障，则通过顺序号触发差错恢复过程

试题（14）分析

X.25 公共数据网 PDN（Public Data Network）是在一个国家或全球范围内提供公共电信服务的数据通信网。X.25 在数据路层采用 LAPB 协议，实际上是 HDLC 的子集，采用了异步平衡方式通信。X.25 的网络层提供面向连接的虚电路服务。有两种形式的虚电路：一种是虚呼叫（Virtual Call，VC），一种是永久虚电路（Permanent Virtual Circuit，PVC）。虚呼叫是动态建立的虚电路，包含呼叫建立、数据传送和呼叫清除等几个过程。永久虚电路是网络指定的固定虚电路，像专线一样，无需建立和释放连接，可直接传送数据。

无论是虚呼叫或是永久虚电路，都是由几条虚拟连接共享一条物理信道。一对分组交换机之间至少有一条物理链路，几条虚电路可以共享该物理链路。每一条虚电路由相邻结点之间的一对缓冲区实现，这些缓冲区被分配给不同的虚电路号以示区别。建立虚电路的过程就是在沿线各结点上分配缓冲区和虚电路号的过程。

通过预先建立的虚电路通信，可以进行端到端的流量和差错控制。X.25 分组头中带有发送顺序号和应答顺序号。如果出现差错，则可以通过顺序号进行纠正。

参考答案

（14）D

试题（15）

使用海明码进行纠错，7 位码长（$x_1x_2x_3x_4x_5x_6x_7$），其中 4 位数据位，3 位校验位，其监督关系式为

$c_0 = x_1 + x_3 + x_5 + x_7$

$c_1 = x_2 + x_3 + x_6 + x_7$

$c_2 = x_4 + x_5 + x_6 + x_7$

如果收到的码字为 1000101，则纠错后的码字是__（15）__。

（15）A．1000001　　B．1001101　　C．1010101　　D．1000101

试题（15）分析

如果收到的码字为 1000101，根据监督关系式计算得到 $c_2c_1c_0$=011，可知错误在第 3 位，则纠错后得到正确的码字为 1010101。

参考答案

（15）C

试题（16）

虚拟局域网中继协议（VTP）有三种工作模式，即服务器模式、客户机模式和透明模式，以下关于这 3 种工作模式的叙述中，不正确的是__（16）__。

（16）A．在服务器模式可以设置 VLAN 信息

B．在服务器模式下可以广播 VLAN 配置信息

C．在客户机模式下不可以设置 VLAN 信息

D．在透明模式下不可以设置 VLAN 信息

试题（16）分析

VLAN 中继协议（VLAN Trunking Protocol，VTP）是 Cisco 公司的专利协议。VTP 在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为 3 种：

① 服务器模式（Server）：交换机在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

② 客户机模式（Client）：在此模式下不允许创建、修改或删除 VLAN，但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

③ 透明模式（Transparent）：在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 帧，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

VTP 协议的优点有：

（1）提供通过一个交换机在整个管理域中配置 VLAN 的方法；

（2）提供跨不同介质类型（如 ATM、FDDI 和以太网）配置 VLAN 的方法；

（3）提供跟踪和监视 VLAN 配置的方法；

（4）保持 VLAN 配置的一致性。

参考答案

（16）D

试题（17）

千兆以太网标准 802.3z 定义了一种帧突发方式，这种方式是指__（17）__。

（17）A. 一个站可以突然发送一个帧

B. 一个站可以不经过竞争就启动发送过程

C. 一个站可以连续发送多个帧

D. 一个站可以随机地发送紧急数据

试题（17）分析

1996 年 3 月 IEEE 成立了 802.3z 工作组，开始制定 1000Mb/s 以太网标准。后来又成立了有 100 多家公司参加的千兆以太网联盟 GEA（Gibabit Ethernet Alliance），支持 IEEE 802.3z 工作组的各项活动。1998 年 6 月公布的 IEEE 802.3z 和 1999 年 6 月公布的 IEEE 802.3ab 已经成为千兆以太网的正式标准。实现千兆数据速率需要采用新的数据处理技术。首先是最小帧长需要扩展，以便在半双工的情况下增加跨距。另外 802.3z 还定义了一种帧突发方式（ frame bursting），使得一个站可以连续发送多个帧。最后物理层编码也采用了与 10Mb/s 不同的编码方法，即 4b/5b 或 8b/9b 编码法。

参考答案

（17）C

试题（18）

以太网最大传输单元（MTU）为 1500 字节。以太帧包含前导（preamble）、目标地址、源地址、协议类型、CRC 等字段，共计 26 个字节的开销。假定 IP 头长为 20 字节，TCP 头长为 20 字节，则 TCP 数据最大为__（18）__字节。

（18）A. 1434　　B. 1460　　C. 1480　　D. 1500

试题（18）分析

由于以太网 MTU 为 1500 字节，从中减去 IP 头 20 个字节和 TCP 头 20 个字节，则允许的 TCP 数据最多为 1460 个字节。

参考答案

（18）B

试题（19）

以下关于网络控制的叙述，正确的是__（19）__。

（19）A. 由于 TCP 的窗口大小是固定的，所以防止拥塞的方法只能是超时重发

B. 在前向纠错系统中，当接收端检测到错误后就要请求发送端重发出错分组

C. 在滑动窗口协议中，窗口的大小以及确认应答使得可以连续发送多个数据

D. 在数据报系统中，所有连续发送的数据都可以沿着预先建立的虚通路传送

试题（19）分析

TCP 采用可变大小的滑动窗口协议进行流量控制。在前向纠错系统中，当接收端检测到错误后就根据纠错编码的规律自行纠错；在后向纠错系统中，接收方会请求发送方重发出错分组。IP 协议不预先建立虚电路，而是对每个数据报独立地选择路由并一站一站地进行转发，直到送达目标地。

参考答案

（19）C

试题（20）

IETF 定义的多协议标记交换（MPLS）是一种第三层交换技术。MPLS 网络由具有 IP 功能、并能执行标记分发协议（LDP）的路由器组成。负责为网络流添加和删除标记的是__（20）__。

（20）A. 标记分发路由器　　B. 标记边缘路由器
C. 标记交换路由器　　D. 标记传送路由器

试题（20）分析

IETF 开发的多协议标记交换 MPLS（Multiprotocol Label Switching）把第 2 层的链路状态信息（带宽、延迟、利用率等）集成到第 3 层的协议数据单元中，从而简化和改进了第 3 层分组的交换过程。理论上，MPLS 支持任何第 2 层和第 3 层协议。MPLS 包头的位置界于第 2 层和第 3 层之间，可称为第 2.5 层。MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包、甚至 ATM 信元等。可以承载 MPLS 的第 2 层协议可以是 PPP、以太帧、ATM 和帧中继等。

当分组进入 MPLS 网络时，标记边缘路由器（Label Edge Router，LER）就为其加上一个标记，这种标记不仅包含了路由表项中的信息（目标地址、带宽、延迟等），而且还引用了 IP 头中的源地址字段、传输层端口号、服务质量等。这种分类一旦建立，分组就被指定到对应的标记交换通路（Label Switch Path，LSP）中，标记交换路由器（Label Switch Router，LSR）将根据标记来处置分组，不再经过第 3 层转发，从而加快了网络的传输速度。

参考答案

（20）B

试题（21）、（22）

HDLC 是一种__（21）__协议，它所采用的流量控制技术是__（22）__。

（21）A. 面向比特的同步链路控制　　B. 面向字节计数的异步链路控制
C. 面向字符的同步链路控制　　D. 面向比特流的异步链路控制

（22）A. 固定大小的滑动窗口协议　　B. 可变大小的活动窗口协议
C. 停等协议　　D. 令牌控制协议

试题（21）、（22）分析

数据链路控制协议可分为两大类：面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，用 10 个专用字符（例如 STX、ETX、ACK、NAK 等）控制传输过程。面向比特的协议以比特作为传输的基本单位，它的传输效率高，能适应计算机通信技术的最新发展，已广泛应用于公用数据网中。面向比特的同步链路控制协议 HDLC 是国际标准化组织（ISO）根据 IBM 公司的 SDLC（Synchronous Data Link Control）协议扩充开发而成的。HDLC 协议采用固定大小的滑动窗口协议实现链路两端的流量和差错控制。

参考答案

（21）A （22）A

试题（23）、（24）

ADSL 采用（23）技术在一对铜线上划分出多个信道，分别传输上行和下行数据以及话音信号。ADSL 传输的最大距离可达（24）米。

（23）A．时分多路 B．频分多路 C．波分多路 D．码分多址

（24）A．500 B．1000 C．5000 D．10000

试题（23）、（24）分析

ADSL 采用时分多路复用技术在一对铜线上划分出多个信道，分别传输上行和下行数据以及话音信号。支持上行速率 640Kb/s～1Mb/s、下行速率 1Mb/s～8Mb/s，有效传输距离在 3～5 公里范围以内，同时还可以提供话音服务。可以满足网上冲浪和视频点播等应用对带宽的要求。

参考答案

（23）B （24）C

试题（25）

按照网络分级设计模型，通常把局域网设计为 3 层，即核心层、汇聚层和接入层，以下关于分级网络功能的描述中，不正确的是（25）。

（25）A．核心层承担访问控制列表检查

B．汇聚层定义了网络的访问策略

C．接入层提供网络接入功能

D．在接入层可以使用集线器代替交换机

试题（25）分析

层次型局域网结构将局域网络划分成不同的功能层次，例如划分成核心层、汇聚层和接入层，通过与核心设备互连的路由器接入广域网，层次结构的特点如下：

（1）网络功能划分清晰，有利发挥联网设备的最大效率；

（2）网络拓扑结构使得故障定位可分级进行，便于维护；

（3）便于网络拓扑的后续扩展。

在三层模型中，核心层提供不同区域之间的高速连接和最优传输路径，汇聚层提供网络业务接入，并实现与安全、流量和路由相关的控制策略，接入层为终端用户提供接入服务。

① 核心层设计要点

核心层是互连网络的高速主干网，在设计中应增加冗余组件，使其具备高可靠性，能快速适应通信流量的变化。

在设计核心层设备的功能时应避免使用数据包过滤、策略路由等降低转发速率的功能特性，使得核心层具有高速率、低延迟和良好的可管理性。

核心层设备覆盖的地理范围不宜过大，连接的设备不宜过多，否则会使得网络的复杂度增大，导致网络性能降低。

核心层应包括一条或多条连接外部网络的专用链路，使得可以高效地访问互联网。

② 汇聚层设计要点

汇聚层是核心层与接入层之间的分界点，应实现资源访问控制和流量控制等功能。汇聚层应该对核心层隐藏接入层的详细信息，不管划分了多少个子网，汇聚层向核心路由器发布路由通告时，只通告各个子网汇聚后的超网地址。

如果局域网中运行了以太网和弹性分组环等不同类型的子网，或者运行了不同路由算法的区域网络，可以通过汇聚层设备完成路由汇总和协议转换功能。

③ 接入层设计要点

接入层提供网络接入服务，并解决本地网段内用户之间互相访问的需求，要提供足够的带宽，使得本地用户之间可以高速访问；

接入层还应提供一部分管理功能，例如 MAC 地址认证、用户认证、计费管理等；

接入层要负责收集用户信息（例如用户 IP 地址、MAC 地址、访问日志等），作为计费和排错的依据。

参考答案

（25）A

试题（26）

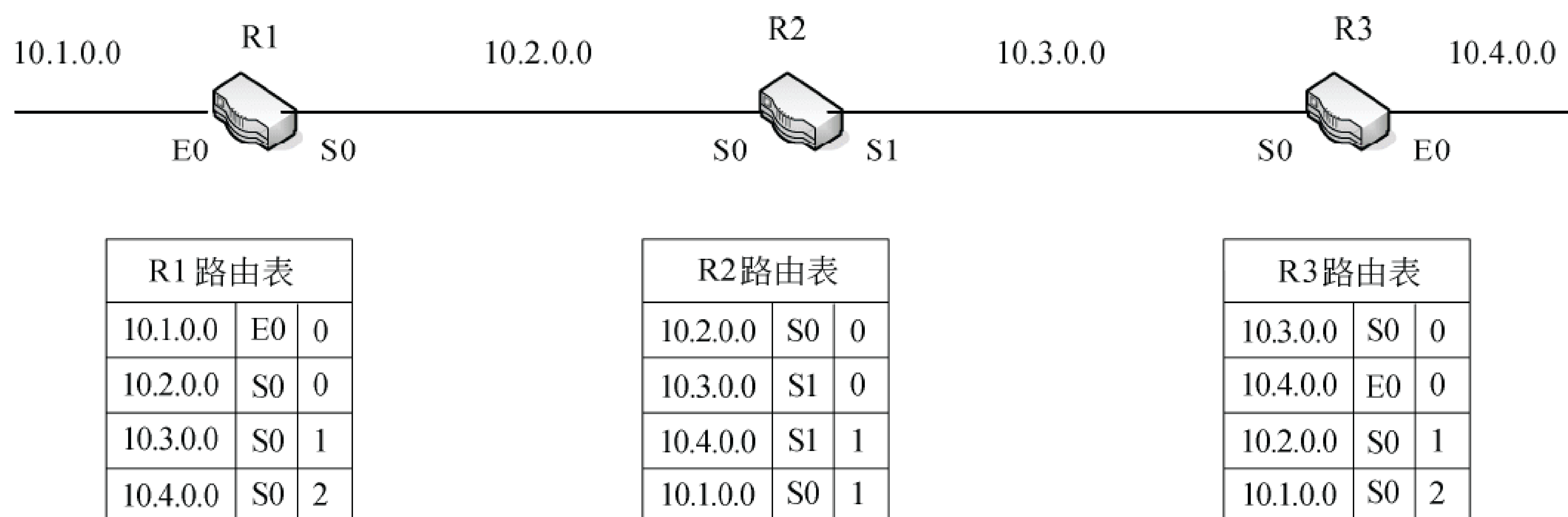
在距离矢量路由协议中，防止路由循环的方法通常有以下三种：<u>（26）</u>。

（26）A. 水平分裂、垂直翻转、设置最大度量值
B. 水平分裂、设置最大度量值、反向路由中毒
C. 垂直翻转、设置最大度量值、反向路由中毒
D. 水平分裂、垂直翻转、反向路由中毒

试题（26）分析

距离矢量法算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路（Routing Loops），使得各个路由器无法就网络的可到达性取得一致。

例如在下图中，路由器 R1、R2、R3 的路由表已经收敛，每个路由表的后两项是通过交换路由信息学习到的。如果在某一时刻，网络 10.4.0.0 发生故障，R3 检测到故障，并通过接口 S0 把故障通知 R2。然而，如果 R2 在收到 R3 的故障通知前将其路由表发送到 R3，则 R3 会认为通过 R2 可以访问 10.4.0.0，并据此将路由表中第二条记录修改为（10.4.0.0，S0，2）。这样一来，路由器 R1、R2、R3 都认为通过其他的路由器存在一条通往 10.4.0.0 的路径，结果导致目标地址为 10.4.0.0 的数据包在三个路由器之间来回传递，从而形成路由环路，直到路由度量达到最大值才能发现网络故障。



R1 路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

R2 路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

R3 路由表		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

解决路由环路问题可以采用水平分割法（Split Horizon）。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。可以对上图中 R2 的路由表项将加上一些注释，这样，每一条路由信息都不会通过其来源接口向回发送，就可以避免环路的产生。

R2 路由表			
10.2.0.0	S0	0	不发送给 R1
10.3.0.0	S1	0	不发送给 R3
10.4.0.0	S1	1	不发送给 R3
10.1.0.0	S0	1	不发送给 R1

简单的水平分割方案是："不能把从邻居学习到的路由发送给那个邻居"，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse）是："把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居"。采用反向毒化的方案更安全一些，它可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

另外，采用触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器 R3 在接收 R2 的更新报文之前把网络 10.4.0.0 的故障告诉 R2，则也可以防止环路的形成。

参考答案

（26）B

试题（27）

以下关于 OSPF 协议的说法中，正确的是＿（27）＿。

（27）A．OSPF 是一种应用于不同自治系统之间外部网关协议
B．OSPF 是基于相邻结点的负载来计算最佳路由
C．在 OSPF 网络中，不能根据网络的操作状态动态改变路由
D．在 OSPF 网络中，根据链路状态算法确定最佳路由

试题（27）分析

OSPF（Open Shortest Path First）是一种内部网关协议，用于在自治系统内进行路由决策。OSPF 是链路状态协议，通过路由器之间通告链路的状态来建立链路状态数据库，根据链路状态算法确定最佳路由，并构造路由表。

OSPF 网络是分层次的，把自治系统内部分为多个区域（Area），每一个区域有它自己的链路状态数据库和拓扑结构图，区域内部的路由器共享相同的路由信息。具有多个接口的路由器可以连接多个区域，这种路由器称为区域边缘路由器，它要为每个相连的区域分别保存一份链路状态数据库。

区域的划分产生了两类不同的 OSPF 路由，区别在于源和目的是在同一区域还是不同的区域，分别称为区域内路由和跨区域路由。

OSPF 路由器之间通过链路状态公告（Link State Advertisement，LSA）交换网络拓扑信息。LSA 中包含连接的接口、链路的度量值（Metric）等信息。

OSPF 路由器启动后以固定的时间间隔泛洪传播 Hello 报文，采用目标地址 224.0.0.5 代表所有的 OSPF 路由器。在点对点网络上每 10 秒发送一次，在 NBMA 网络中每 30 秒发送一次。管理 Hello 报文交换的规则称为 Hello 协议。Hello 协议用于发现邻居，建立毗邻关系，还用于选举区域内的指定路由器 DR 和备份指定路由器 BDR。

在正常情况下，区域内的路由器与本区域的 DR 和 BDR 通过互相发送数据库描述报文（DBD）交换链路状态信息。路由器把收到的链路状态信息与自己的链路状态数据库进行比较，如果发现接收到了不在本地数据库中的链路信息，则向其邻居发送链路状态请求报文 LSR，要求传送有关该链路的完整更新信息。接收到 LSR 的路由器用链路状态更新 LSU 报文响应，其中包含了有关的链路状态通告 LSA。

参考答案

（27）D

试题（28）

以下关于外部网关协议 BGP4 的说法，错误的是＿（28）＿。

（28）A．BGP4 是一种路径矢量路由协议　　B．BGP4 通过 UDP 传输路由信息
C．BGP4 支持路由汇聚功能　　D．BGP4 能够检测路由循环

试题（28）分析

外部网关协议 BGP4 已经广泛地应用于不同 ISP 的网络之间，成为事实上的 Internet 外部路由协议标准。BGP 4 是一种动态路由发现协议，支持无类别域间路由 CIDR。BGP 的主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 报文通过 TCP（179 端口）连接传送。

BGP 是一种路径矢量路由协议，BGP 路由器之间传送的路由信息由一个目标地址前缀后随一串 AS 编号组成，通过检测路径中是否出现本地 AS 编号可以发现路由循环。BGP 路由器根据收到的各个路径矢量和预订的管理策略，选择到达目标的最短通路，可见 BGP 与 RIP 协议的算法是相似的。

参考答案

（28）B

试题（29）

与 HTTP1.0 相比，HTTP 1.1 最大的改进在于__（29）__。

（29）A．进行状态保存　　B．支持持久连接
　　　C．采用 UDP 连接　　D．提高安全性

试题（29）分析

本题考查 HTTP 协议及相关技术。

HTTP 1.0 协议使用非持久连接，在非持久连接下，一个 TCP 连接只传输一个 Web 对象。HTTP/1.1 默认使用持久连接（HTTP/1.1 协议的客户机和服务器可以配置成使用非持久连接），在持久连接下，不必为每个 Web 对象的传送建立一个新的连接，一个连接中可以传输多个对象。

参考答案

（29）B

试题（30）～（33）

网管中心在进行服务器部署时应充分考虑到功能、服务提供对象、流量、安全等因素。某网络需要提供的服务包括 VOD 服务、网络流量监控服务以及可对外提供的 Web 服务和邮件服务。在对以上服务器进行部署过程中，VOD 服务器部署在__（30）__； Web 服务器部署在__（31）__；流量监控器部署在__（32）__，这四种服务器中通常发出数据流量最大的是__（33）__。

（30）A．核心交换机端口　　B．核心交换机镜像端口
　　　C．汇聚交换机端口　　D．防火墙 DMZ 端口

（31）A．核心交换机端口　　B．核心交换机镜像端口
　　　C．汇聚交换机端口　　D．防火墙 DMZ 端口

（32）A．核心交换机端口　　B．核心交换机镜像端口
　　　C．汇聚交换机端口　　D．防火墙 DMZ 端口

（33）A. VOD 服务器　　B. 网络流量监控服务器
C. Web 服务器　　D. 邮件服务器

试题（30）～（33）分析

本题考查服务器部署及相关技术。

在进行服务器部署时，应充分考虑到功能，服务提供对象，流量、安全等因素。VOD 服务器流量较大，应部署在核心交换机端口。Web 服务器需对外提供服务，一般部署在防火墙 DMZ 端口。网络流量监控需要监听交换网络中所有流量，但是通过普通交换机端口去获取这些流量有相当大的困难，因此需要通过配置交换机来把一个或多个端口（VLAN）的数据转发到某一个端口来实现对网络的监听，这个端口就是镜像端口，而网络流量监控服务器需要部署在镜像端口。

参考答案

（30）A　（31）D　（32）B　（33）B

试题（34）

可提供域名服务的包括本地缓存、本地域名服务器、权限域名服务器、顶级域名服务器以及根域名服务器等，以下说法中错误的是__（34）__。

（34）A. 本地缓存域名服务不需要域名数据库
B. 顶级域名服务器是最高层次的域名服务器
C. 本地域名服务器可以采用递归查询和迭代查询两种查询方式
D. 权限域名服务器负责将其管辖区内的主机域名转换为该主机的 IP 地址

试题（34）分析

本题考查域名服务器及相关技术。

可提供域名服务的包括本地缓存、本地域名服务器、权限域名服务器、顶级域名服务器以及根域名服务器。DNS 主机名解析的查找顺序是，先查找客户端本地缓存；如果没有成功，则向 DNS 服务器发出解析请求。

本地缓存是内存中的一块区域，保存着最近被解析的主机名及其 IP 地址映像。由于解析程序缓存常驻内存中，所以比其他解析方法速度快。

当一个主机发出 DNS 查询报文时，这个查询报文就首先被送往该主机的本地域名服务器。本地域名服务器离用户较近，当所要查询的主机也属于同一个本地 ISP 时，该本地域名服务器立即就能将所查询的主机名转换为它的 IP 地址，而不需要再去询问其他的域名服务器。

每一个区都设置有域名服务器，即权限服务器，它负责将其管辖区内的主机域名转换为该主机的 IP 地址。在其上保存有所管辖区内的所有主机域名到 IP 地址的映射。

顶级域名服务器负责管理在本顶级域名服务器上注册的所有二级域名。当收到 DNS 查询请求时，能够将其管辖的二级域名转换为该二级域名的 IP 地址。或者是下一步应该找寻的域名服务器的 IP 地址。

根域名服务器是最高层次的域名服务器。每一个根域名服务器都要存有所有顶级域名服务器的 IP 地址和域名。当一个本地域名服务器对一个域名无法解析时，就会直接找到根域名服务器，然后根域名服务器会告知它应该去找哪一个顶级域名服务器进行查询。

参考答案

（34）B

试题（35）、（36）

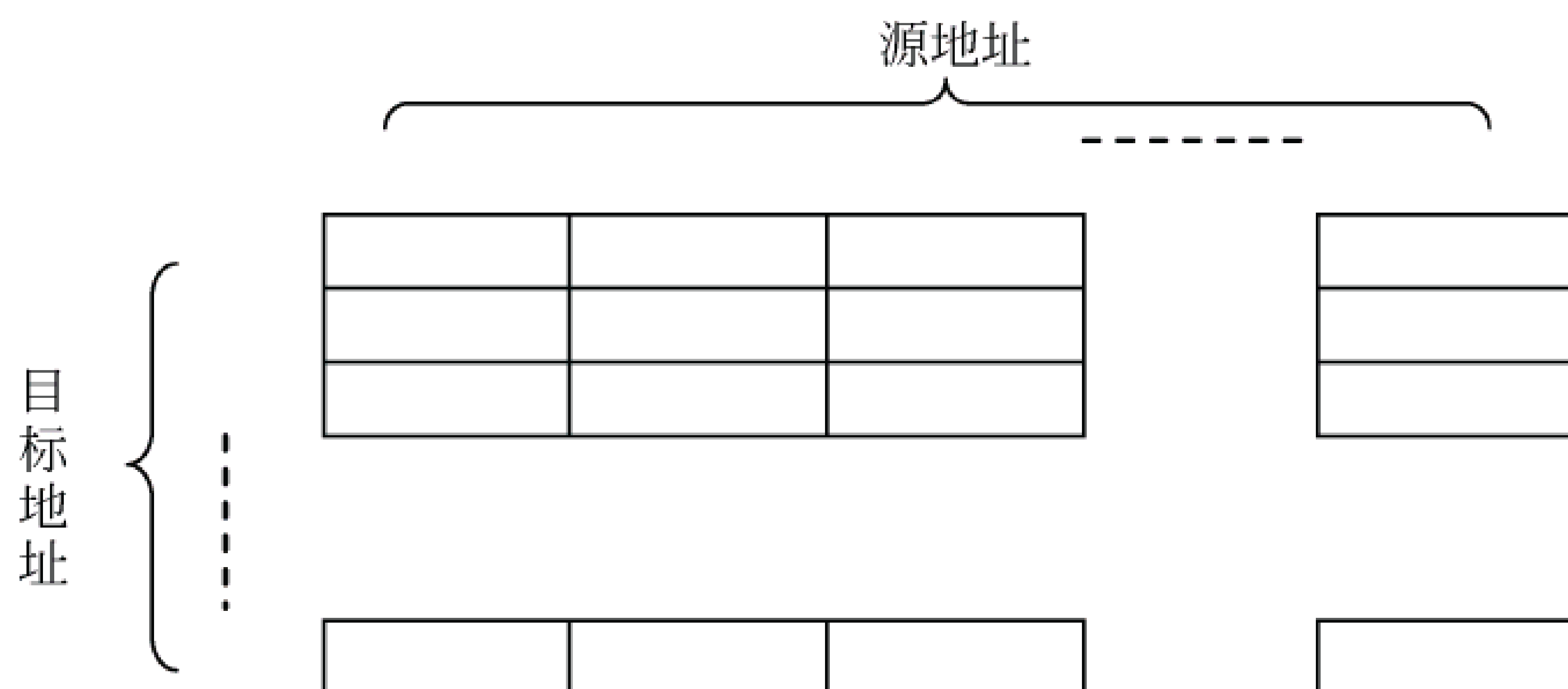
在 RMON 管理信息库中，矩阵组存储的信息是＿（35）＿，警报组的作用是＿（36）＿。

（35）A. 一对主机之间建立的 TCP 连接数　　B. 一对主机之间交换的字节数
　　　C. 一对主机之间交换的 IP 分组数　　D. 一对主机之间发生的冲突次数

（36）A. 定义了一组网络性能门限值　　B. 定义了网络报警的紧急程度
　　　C. 定义了网络故障的处理方法　　D. 定义了网络报警的受理机构

试题（35）、（36）分析

矩阵组记录了子网中一对主机之间的通信量，信息以矩阵的形式存储，如下图所示。



如果监视器在某个接口上发现了一对主机会话，则在该表中记录两行，每行表示一个方向的通信量。这样，管理站可以检索到一个主机向其他主机发送的信息，也容易检索到其他主机向某一个主机发送的信息。

RMON 报警组定义了一组有关网络性能的门限值，超过门限值时向控制台产生报警事件。报警组由一个表组成，该表的一行定义了一种报警：监视的变量、采样区间和门限值。

参考答案

（35）B　（36）A

试题（37）

设有下面 4 条路由：172.118.129.0/24、172.118.130.0/24、172.118.132.0/24 和 172.118.133.0/24，如果进行路由汇聚，能覆盖这 4 条路由的地址是＿（37）＿。

（37）A. 172.118.128.0/21　　B. 172.118.128.0/22
　　　C. 172.118.130.0/22　　D. 172.118.132.0/20

试题（37）分析

地址 172.118.129.0/24 的二进制形式为：10101100 01110110 10000001 00000000。

地址 172.118.130.0/24 的二进制形式为：10101100 01110110 10000010 00000000。

地址 172.118.132.0/24 的二进制形式为：10101100 01110110 10000100 00000000。

地址 172.118.133.0/24 的二进制形式为：10101100 01110110 10000101 00000000。

地址 172.118.128.0/21 的二进制形式为：10101100 01110110 10000000 00000000。

所以能覆盖这 4 条路由的地址是 172.118.128.0/21。

参考答案

（37）A

试题（38）

属于网络 202.117.200.0/21 的地址是＿（38）＿。

（38）A．202. 117. 198. 0　　B．202. 117. 206. 0

C．202. 117. 217. 0　　D．202. 117. 224. 0

试题（38）分析

地址 202.117.200.0/21 的二进制形式为：11001010 01110101 11001000 00000000。

202. 117. 198. 0 的二进制形式为：11001010 01110101 11000110 00000000。

202. 117. 206. 0 的二进制形式为：11001010 01110101 11001110 00000000。

202. 117. 217. 0 的二进制形式为：11001010 01110101 11011001 00000000。

202. 117. 224. 0 的二进制形式为：11001010 01110101 11100000 00000000。

可以看出 202. 117. 206. 0 属于网络 202.117.200.0/21。

参考答案

（38）B

试题（39）

下面的地址中，属于单播地址的是＿（39）＿。

（39）A．172.31.128.255/18　　B．10.255.255.255

C．172.160.24.59/30　　D．224.105.5.211

试题（39）分析

地址 172.31.128.255/18 的二进制形式是 10101100 00011111 10000000 11111111

可见是一个单播地址。

地址 10.255.255.255 是 A 类网络定向广播地址。

地址 172.160.24.59/30 的二进制形式是 10101100 10100000 00011000 00111011

可见是一个广播地址。

地址 224.105.5.211D 类组播地址。

参考答案

（39）A

试题（40）

在 IPv6 中，地址类型是由格式前缀来区分的。IPv6 可聚合全球单播地址的格式前缀是 （40） 。

（40）A．001 B．1111 1110 10 C．1111 1110 11 D．1111 1111

试题（40）分析

IPv6 地址的格式前缀（Format Prefix，FP）用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可表示为“IPv6 地址/前缀长度”的形式。例如 60 位的地址前缀 12AB00000000CD3 有下列几种合法的表示形式：

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

IPv6 地址的具体类型是由格式前缀来区分的，这些前缀的初始分配如下表所示。

分　　配	前缀（二进制）	占地址空间的比例
保留	0000 0000	1/256
未分配	0000 000	11/256
为 NSAP 地址保留	0000 001	1/128
为 IPX 地址保留	0000 010	1/128
未分配	0000 011	1/128
未分配	0000 1	1/32
未分配	0001	1/16
可聚合全球单播地址	001	1/8
未分配	010	1/8
未分配	011	1/8
未分配	100	1/8
未分配	101	1/8
未分配	110	1/8
未分配	1110	1/16
未分配	1111 0	1/32
未分配	1111 10	1/64
未分配	1111 110	1/128
未分配	1111 1110 0	1/512
链路本地单播地址	1111 1110 10	1/1024
站点本地单播地址	1111 1110 11	1/1024
组播地址	1111 1111	1/256

参考答案

（40）A

试题（41）

SSL 包含的主要子协议是记录协议、__（41）__。

（41）A．AH 协议和 ESP 协议　　B．AH 协议和握手协议
C．警告协议和 ESP 协议　　D．警告协议和握手协议

试题（41）分析

本题考查网络安全方面关于安全协议 SSL 的基础知识。

SSL 协议主要包括记录协议、警告协议和握手协议。

记录协议用于在客户机和服务器之间交换应用数据；告警协议用来为对等实体传递 SSL 的相关警告。用于标示在什么时候发生了错误或两个主机之间的会话在什么时候终止；握手协议用于产生会话状态的密码参数，允许服务器和客户机相互验证、协商加密和 MAC 算法及秘密密钥，用来保护在 SSL 记录中传送的数据。

参考答案

（41）D

试题（42）

SET 安全电子交易的整个过程不包括__（42）__阶段。

（42）A．持卡人和商家匹配　　B．持卡人和商家注册
C．购买请求　　D．付款授权和付款结算

试题（42）分析

本题考查网络安全方面关于安全协议 SET 的基础知识。

SET 安全电子交易的整个过程大体可分为以下几个阶段：持卡人注册、商家注册、购买请求、付款授权和付款结算。

参考答案

（42）A

试题（43）

下列访问控制模型中，对象的访问权限可以随着执行任务的上下文环境发生变化的是__（43）__的控制模型。

（43）A．基于角色　　B．基于任务　　C．基于对象　　D．强制型

试题（43）分析

本题考查网络安全方面关于访问控制模型的基础知识。

强制型访问控制（MAC）模型是一种多级访问控制策略，它的主要特点是系统对访问主体和受控对象实行强制访问控制，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。

基于角色的访问控制（RBAC Model，Role-based Access）：RBAC 模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许

可权。

基于任务的访问控制模型（TBAC Model，Task-based Access Control Model）是从应用和企业层角度来解决安全问题，以面向任务的观点，从任务（活动）的角度来建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。在 TBAC 中，对象的访问权限控制并不是静止不变的，而是随着执行任务的上下文环境发生变化。

基于对象的访问控制模型（OBAC Model：Object-based Access Control Model）中，将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合；同时允许对策略和规则进行重用、继承和派生操作。

参考答案

（43）B

试题（44）

数字证书被撤销后存放于＿（44）＿。

（44）A．CA　　B．CRL　　C．ACL　　D．RA

试题（44）分析

本题考查网络安全方面关于数字证书的基础知识。

CLR（Certificate Revocation List）的全称是证书撤销列表，用于保存被撤销的数字证书。

参考答案

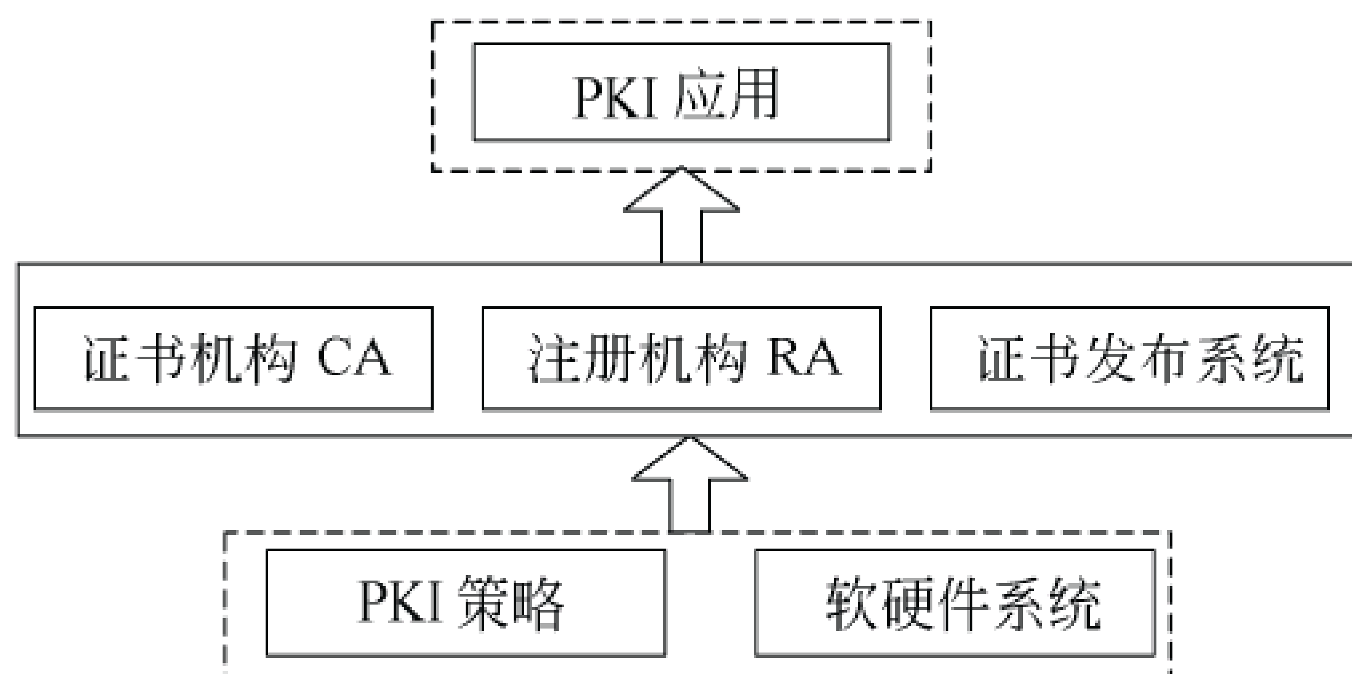
（44）B

试题（45）、（46）

下图所示 PKI 系统结构中，负责生成和签署数字证书的是＿（45）＿，负责验证用户身份的是＿（46）＿。

（45）A．证书机构 CA　　B．注册机构 RA
　　C．证书发布系统　　D．PKI 策略

（46）A．证书机构 CA　　B．注册机构 RA
　　C．证书发布系统　　D．PKI 策略



试题（45）、（46）分析

本题考查网络安全方面关于 PKI 的基础知识。

在 PKI 系统体系中，证书机构 CA 负责生成和签署数字证书，注册机构 RA 负责验证申请数字证书用户的身份。

参考答案

（45）A　（46）B

试题（47）

以下关于完美向前保护（PFS）的说法，错误的是__（47）__。

（47）A．PFS 的英文全称是 Perfect Forward Secrecy

B．PFS 是指即使攻击者破解了一个密钥，也只能还原这个密钥加密的数据，而不能还原其他的加密数据

C．IPSec 不支持 PFS

D．要实现 PFS 必须使用短暂的一次性密钥

试题（47）分析

本题考查网络安全方面关于 PFS 的基础知识。

完美向前保护 PFS（Perfect Forward Secrecy）是一种密码系统，如果一个密钥被窃取，那么只有被这个密钥加密的数据会被窃取。

在使用 PFS 之前，IPSEC 第二阶段的密钥是从第一阶段的密钥导出的，使用 PFS，使 IPSEC 的两个阶段的密钥是独立的。所以采用 PFS 来提高安全性。

PFS 要求一个密钥只能访问由它所保护的数据；用来产生密钥的元素一次一换，不能再产生其他的密钥，因此一个密钥被破解，并不影响其他密钥的安全性。

参考答案

（47）C

试题（48）

某系统主要处理大量随机数据。根据业务需求，该系统需要具有较高的数据容错性和高速读写性能，则该系统的磁盘系统在选取 RAID 级别时最佳的选择是__（48）__。

（48）A．RAID0　B．RAID1　C．RAID3　D．RAID10

试题（48）分析

本题考查 RAID 的基础知识。RAID 是由一个硬盘控制器来控制多个硬盘的相互连接，使多个硬盘的读写同步，减少错误，增加效率和可靠度的技术。RAID 技术经过不断的发展，现在已拥有了从 RAID 0 到 6 七种基本的 RAID 级别。另外，还有一些基本 RAID 级别的组合形式，如 RAID 10（RAID 0 与 RAID 1 的组合），RAID 50（RAID 0 与 RAID 5 的组合）等。其中，RAID 0 特别适用于对性能要求较高，而对数据安全要求低的领域；RAID 1 提供最高的数据安全保障，但由于数据是完全备份所以磁盘空间利用率低，速度不高；RAID3 比较适合大文件类型且安全性要求较高的应用，如视频编辑、硬盘播出机、大型数据库等；RAID 10 特别适用于既有大量随机数据需要存取，同时又对数据安全性要求严格的领域，如银行、金融、商业超市、仓储库房、各种档案管理等。

参考答案

（48）D

试题（49）

以下关于网络存储描述正确的是＿（49）＿。

（49）A．DAS 支持完全跨平台文件共享，支持所有的操作系统

B．NAS 是通过 SCSI 线接在服务器上，通过服务器的网卡向网络上传输数据

C．FC SAN 的网络介质为光纤通道，而 IP SAN 使用标准的以太网

D．SAN 设备有自己的文件管理系统，NAS 中的存储设备没有文件管理系统

试题（49）分析

本题考查网络存储的基础知识。

DAS（Direct Attached Storage，直接附加存储）即直连方式存储。在这种方式中，存储设备是通过电缆（通常是 SCSI 接口电缆）直接连接服务器。I/O（输入/输出）请求直接发送到存储设备。DAS 也可称为 SAS（Server-Attached Storage，服务器附加存储）。它依赖于服务器，其本身是硬件的堆叠，不带有任何存储操作系统， DAS 不能提供跨平台文件共享功能，各系统平台下文件需分别存储。

NAS 是（Network Attached Storage）的简称，中文称为网络附加存储。在 NAS 存储结构中，存储系统不再通过 I/O 总线附属于某个特定的服务器或客户机，而是直接通过网络接口与网络直接相连，由用户通过网络来访问。

NAS 设备有自己的 OS，其实际上是一个带有瘦服务的存储设备，其作用类似于一个专用的文件服务器，不过把显示器，键盘，鼠标等设备省去，NAS 用于存储服务，可以大大降低了存储设备的成本，另外 NAS 中的存储信息都是采用 RAID 方式进行管理的，从而有效地保护了数据。

SAN 是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统，未来的信息存储将以 SAN 存储方式为主。SAN 主要采取数据块的方式进行数据和信息的存储，目前主要使用于以太网（IP SAN）和光纤通道（FC SAN）两类环境中。

参考答案

（49）C

试题（50）

某单位使用非 intel 架构的服务器，要对服务器进行远程监控管理需要使用＿（50）＿。

（50）A．EMP　　B．ECC　　C．ISC　　D．SMP

试题（50）分析

本题考查服务器远程监控管理的基础知识。上述技术中的概念如下：

EMP（Emergency Management Port）技术是一种远程管理技术，利用 EMP 技术可以在客户端通过电话线或电缆直接连接到服务器，来对服务器实施异地操作，如关闭操作系统、启动电源、关闭电源、捕捉服务器屏幕、配置服务器 BIOS 等操作，是一种很

好的实现快速服务和节省维护费用的技术手段。

ECC（Error Checking and Correcting，错误检查和纠正）不是一种内存类型，只是一种内存技术。ECC 纠错技术也需要额外的空间来储存校正码，但其占用的位数跟数据的长度并非成线性关系。

ISC（Intel Server Control，Intel 服务器控制）是一种网络监控技术，只适用于使用 Intel 架构的带有集成管理功能主板的服务器。采用这种技术后，用户在一台普通的客户机上，就可以监测网络上所有使用 Intel 主板的服务器，监控和判断服务器是否“健康”。一旦服务器中机箱、电源、风扇、内存、处理器、系统信息、温度、电压或第三方硬件中的任何一项出现错误，就会报警提示管理人员。

SMP（Symmetrical MultiProcessing，对称多处理）技术是相对非对称多处理技术而言的、应用十分广泛的并行技术。在这种架构中，多个处理器运行操作系统的单一复本，并共享内存和一台计算机的其他资源。所有的处理器都可以平等地访问内存、I/O 和外部中断。

参考答案

（50）A

试题（51）

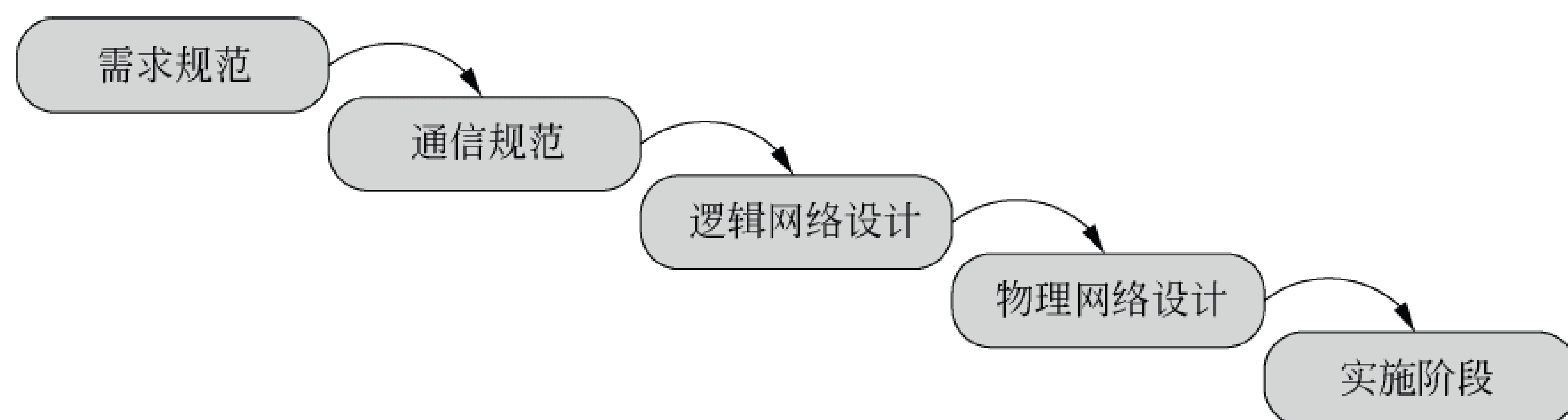
五阶段周期是较为常见的迭代周期划分方式，将网络生命周期的一次迭代划分为需求规范、通信规范、逻辑网络设计、物理网络设计和实施阶段共五个阶段。其中搭建试验平台、进行网络仿真是<u>（51）</u>阶段的任务。

（51）A．需求规范　　B．逻辑网络设计
C．物理网络设计　　D．实施阶段

试题（51）分析

本题考查网络规划设计生命周期及各阶段任务。

五阶段周期是较为常见的迭代周期划分方式，将一次迭代划分为五个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计以及实施阶段，其“瀑布模型”，形成了特定的工作流程，如下图所示。



逻辑设计阶段主要完成网络的逻辑拓扑结构、网络编址、设备命名、交换及路由协议选择、安全规划、网络管理等设计工作，并且根据这些设计产生对设备厂商、服务提

供商的选择策略。搭建试验平台、进行网络仿真是逻辑网络设计阶段的任务。

参考答案

（51）B

试题（52）

在进行网络开发过程的五个阶段中，IP 地址方案及安全方案是在__（52）__阶段提交的。

（52）A．需求分析　　B．通信规范分析
C．逻辑网络设计　　D．物理网络设计

试题（52）分析

本题考查网络规划设计生命周期及各阶段任务。

IP 地址方案及安全方案是在逻辑网络设计阶段提交的。

参考答案

（52）C

试题（53）

某部队拟建设一个网络，由甲公司承建。在撰写需求分析报告时，与常规网络建设相比，最大不同之处是__（53）__。

（53）A．网络隔离需求　　B．网络性能需求
C．IP 规划需求　　D．结构化布线需求

试题（53）分析

本题考查网络需求分析相关内容。

由于拟建设的是某部队网络，故与常规网络建设相比，安全性是最为重要的考虑因素，网络隔离需求尤其重要。

参考答案

（53）A

试题（54）

采购设备时需遵循一些原则，最后参考的原则是__（54）__。

（54）A．尽可能选取同一厂家的产品，保持设备互连性、协议互操作性、技术支持等优势
B．尽可能保留原有网络设备的投资，减少资金的浪费
C．强调先进性，重新选用技术最先进、性能最高的设备
D．选择性能价格比高、质量过硬的产品，使资金的投入产出达到最大值

试题（54）分析

本题考查设备选型相关内容。

在物理网络设计阶段，根据需求说明书、通信规范说明书和逻辑网络设计说明书选择设备的品牌和型号的工作，是较为关键的任务之一。在进行设备的品牌、型号的选择

时，应该考虑到以下方面的内容：

产品技术指标：产品的技术指标是决定设备选型的关键，所有可以选择的产品，都必须满足依据通信规范分析中产生的技术指标，也必须满足逻辑网络设计中形成的逻辑功能。

成本因素：除了产品的技术指标之外，设计人员和用户最关心的就是成本因素，网络中各种设备的成本主要包括购置成本、安装成本、使用成本。

原有设备的兼容性：在产品选型过程中，与原有设备的兼容性是设计人员必须考虑的内容。

产品的延续性：产品的延续性是设计人员保证网络生命周期的关键因素，产品的延续性主要体现在厂商对某种型号的产品是否继续研发、继续生产、继续保证备品配件供应、继续提供技术服务。

设备可管理性：设备可管理性是进行设备选型时的一个非关键因素，但也是必须考虑的内容。

设备的先进性也是选型时应考虑的要素，但要以考虑上述因素为前提。

参考答案

（54）C

试题（55）

网络设计时主要考虑网络效率，ATM 网络中信元的传输效率为__（55）__。

（55）A．50%　　B．87.5%　　C．90.5%　　D．98.8%

试题（55）分析

本题考查 ATM 网络中信元的传输效率。

网络效率的计算公式为效率=（帧长–帧头和帧尾）/（帧长）×100%，额外开销指不能用于传输用户数据的带宽比例，额外开销=（1–效率）；在 ATM 网络中，由于信元长度固定为 53 个字节，信元头部固定为 5 个字节，因此，ATM 的网络效率为（53–48）/ 53×100%=90.5%，额外开销=1–90.5%=9.5%；在传统以太网络中，由于以太网的帧头大小固定，而用户数据不固定，但有最小帧长和最大帧长，因此以太网的最小网络效率为（64–18）/ 64×100%=87.5%，最大额外开销为 12.5%，最大网络效率为（1518–18）/ 1518×100%=98.8%，最小额外开销为 0.02%，实际应用中，要根据以太网的平均帧长来计算平均网络效率。

参考答案

（55）C

试题（56）

在网络设计时需进行网络流量分析。以下网络服务中从客户机至服务器流量比较大的是__（56）__。

（56）A．基于 SNMP 协议的网管服务　　B．视频点播服务

C. 邮件服务　　　　　　D. 视频会议服务

试题（56）分析

本题考查网络设计的基本知识。

在进行网络设计时需进行网络流量分析，在网络流量分析时，要确定系统的业务需求、用户需求、应用需求、网络需求部分的内容，并根据通信流量的分析进行确定。

其中，应用需求要根据通信模式明确各种应用程序的估算使用量。其中，工作邮件、文件共享服务的网络通信模式为客户机-服务器模式，属于双向流量大，因此在网段流量分布上应用的总流量在两个方向上各占 50%，而浏览器-服务器模式，在估算时客户机至服务器按 20%进行估算，反向按 80%进行估算，视频点播属于单播模式，其通讯量主要在服务器到客户机，视频会议系统属于对等模式，服务器到客户机的通讯量基本一致。基于 SNMP 协议的网管服务的通讯主要是客户机向服务器发送相应状态信息，所以在该应用中从客户机至服务器流量比较大。

参考答案

（56）A

试题（57）

在分析网络性能时，__（57）__能有效地反应网络用户之间的数据传输量。

（57）A. 吞吐量　　B. 响应时间　　C. 精确度　　D. 利用率

试题（57）分析

本题考查网络性能分析的基本知识。

在进行网络设计时，对网络性能参数的考虑是设计工作的重点内容之一，需要考虑的网络性能参数包括响应时间、吞吐量、延迟、带宽、容量等。

响应时间是指以计算机或终端向远端资源发出请求时间为起始时间，以该设备接收到数据响应的时间为终点，两个时间之间的差值，这个时间直接影响到用户操作的响应效果，是评估网络用户体验的关键值。

利用率描述设备在使用时所能发挥的最大能力。在网络分析与设计过程中，通常考虑 CPU 利用率和链路利用率。

吞吐量是指在网络用户之间有效地传输数据的能力。如果说数据传输率给出了网络所能传输的比特数，那么吞吐量就是它真正有效的数据传输率。吞吐量常用来评估整个网络的性能。

可用性是指网络或网络设备（如主机或服务器）可用于执行预期任务时间所占总量的百分比。可用性百分值越高，就意味着设备或系统出现故障的可能性越小，提供的正常服务时间越多。

参考答案

（57）A

试题（58）

在分层网络设计中，汇聚层实现__（58）__。

（58）A. 高速骨干线路　　B. 用户认证
　　　C. MAC 绑定　　D. 流量控制

试题（58）分析

本题考查分层网络设计的基本知识。

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定义为核心层、汇聚层、接入层。层次局域网一般通过与核心层设备互连的路由设备接入广域网络，核心层为下两层提供优化的数据转移功能，它是一个高速的交换骨干，其作用是尽可能快地交换数据包而不应卷入到具体数据包的运算中（ACL，过滤等），否则会降低数据包的交换速度。汇聚层提供基于统一策略的互连性，它连接核心层和接入层，对数据包进行复杂的运算。在园区网络环境中，分布层主要提供如下功能：地址的聚集、部门和工作组的接入、广播域；组播传输域的定义 VLAN 分割、介质转换、流量控制等。

接入层的主要功能是为最终用户提供对网络访问的途径。主要提供如下功能：用户接入、带宽共享、交换带宽、MAC 层过滤和网段微分。

参考答案

（58）D

试题（59）

综合布线要求设计一个结构合理、技术先进、满足需求的综合布线系统方案，__（59）__不属于综合布线系统的设计原则。

（59）A. 综合考虑用户需求、建筑物功能、经济发展水平等因素
　　　B. 长远规划思想、保持一定的先进性
　　　C. 不必将综合布线系统纳入建筑物整体规划、设计和建设中
　　　D. 扩展性、标准化、灵活的管理方式

试题（59）分析

本题考查综合布线系统的设计原则。

综合布线系统就是为了顺应发展需求而特别设计的一套布线系统。对于现代化的大楼来说，它采用了一系列高质量的标准材料，以模块化的组合方式，把语音、数据、图像和部分控制信号系统用统一的传输媒介进行综合，经过统一的规划设计，综合在一套标准的布线系统中。综合布线要求设计一个结构合理、技术先进、满足需求的综合布线系统方案，必须综合考虑用户需求、建筑物功能、经济发展水平等因素，长远规划思想、保持一定的先进性，同时将综合布线系统纳入建筑物整体规划、设计和建设中，保持扩展性、标准化、灵活的管理方式。

参考答案

（59）C

试题（60）

传统数据中心机房的机柜在摆放时，为了美观和便于观察会将全部机柜朝同一个方向摆放，但实际上这种做法不是很合理，正确的做法应该是将服务器机柜按照面对面或背对背的方式布置，这样做是为了＿（60）＿。

（60）A．减小楼体荷载　　B．节省服务器资源
C．节能环保　　D．避免电磁干扰

试题（60）分析

本题考查绿色数据中心机房中机柜摆放的相关知识。

在现代机房的机柜布局中，人们为了美观和便于观察会将所有的机柜朝同一个方向摆放，那么如果按照这种摆放方式，机柜盲板有效阻挡冷热空气的效果将大打折扣。这是因为当机柜朝统一方向摆放时就形成了第一排机柜背面正对着第二排机柜的正面，这样两排机柜中间的通道就会出现冷热气流混合循环，形成冷热气流短路致使第二排机柜的冷风进口温度大大提高，严重破坏了冷风通道的环境温度。正确的摆放方式应该是将服务器机柜面对面或背对背的方式摆放，即当机柜内或机架上的设备为前进风/后出风方式冷却时，机柜或机架的布置宜采用面对面、背对背方式。这样便形成了冷风通道和热风通道。机柜之间的冷热风不会混合在一起，形成短路气流，大大提高了制冷效果，保护好了冷热通道不被破坏。

正确的选择制冷设备和机柜，以及合理的机柜布局将大大提高制冷效率，同时也将大大降低了 IT 设备运行的总拥有成本，这也将是绿色数据中心未来设计发展的方向和趋势。

参考答案

（60）C

试题（61）

某公司新建一栋 30 层的大楼，在该楼内设信息系统中心机房时，综合考虑各方面因素，对于中心机房的楼层选址建议位于＿（61）＿。

（61）A．1 层　　B．2 层　　C．5 层　　D．30 层

试题（61）分析

本题考查数据中心机房选址的相关知识。

对于一般的机房选址来说，大楼位置的选择可能很少受机房选址要求的影响，但是楼内机房位置的选择，却是机房使用、规划和设计部门可以认真考虑的。对于多层或高层建筑物内的电子信息系统机房，在确定主机房的位置时，应对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合分析和经济比较；采用机房专用空调的主机房，应具备安装空调室外机的建筑条件。综合考虑以上因素，机房宜设置在大楼的第二、三层

或裙楼的中间层。将机房设置在一楼和地下室虽然从结构荷载、雷电感应、设备搬运等方面考虑有好处，但有水浸、多尘、虫鼠害以及安保方面的担忧。机房设置在大楼的第二、三层或裙楼的中间层既有一层的优点，又克服了一层的缺点，所以是建设机房的最佳楼层，而且对安装空调室外机有更多的选择。如果大楼是高层建筑，且楼下无法安装空调室外机，或因为其他原因无法在大楼低层建设机房，则宜选择在最高层以下的几个楼层，因为顶层保温比较困难，还容易发生漏水事故。

参考答案

（61）B

试题（62）

某大型企业网络出口带宽 1000M，因为各种原因出口带宽不能再扩，随着网络的运行发现访问外网的 Web 以及使用邮件越来越慢，经过分析发现内网 P2P、视频/流媒体、网络游戏流量过大，针对这种情况考虑对网络进行优化，可以采用<u>（62）</u>来保障正常的网络需求。

（62）A．部署流量控制设备　　B．升级核心交换机
　　　C．升级接入交换机　　D．部署网络安全审计设备

试题（62）分析

本题考查网络故障排查的相关知识。

众所周知，网络带宽资源建设的发展速度永远跟不上各种网络应用的增长速度。对企业出口带宽无尽的增长需求势必给企业带来额外的经济负担，所以对企业网络流量进行管理已是迫在眉睫的事情。广义上说安全管理设备也算流控，但其主要用途是记录和控制网络中的用户行为，比如限制用户使用 QQ、玩游戏等等，但其流控功能较弱，一般适用于上网人数较少的场合。由于安全管理设备的应用场景复杂，流控功能和性能并不专业，对带宽的优化能力很弱，采用行为管理设备充当流控设备使用还可能导致网络延迟增大，偶尔还会导致断网现象发生。而专用的流控设备主要目的是优化带宽，通过限制带宽占用能力强的应用以保护关键应用，通过多种复杂的策略来实现合理的带宽分配。专用的流量控制设备通过应用封堵、流量限速等流量限制等手段，控制非关键应用，封堵无关应用，极大地提升现有带宽的利用价值，避免因带宽扩容带来额外的网络接入费用。同时通过数据压缩功能，大大降低了网络中传输的数据量，有效提升了当前的带宽利用价值，避免因额外租用出口带宽资源而增加网络运营成本。因此可以采用部署流量控制设备来保障正常的网络需求。

参考答案

（62）A

试题（63）

某大学 WLAN 无线校园网已经全面覆盖了校园，AP 数量、信号强度等满足覆盖需求。学校无线用户要求接入某运营商的 WLAN，针对现状可采用的最优化技术方案是

（63）____。

（63）A．运营商新建自己的 WLAN 无线网络
B．运营商利用学校现有无线网络，在 AP 上增加一个自己的 SSID
C．运营商利用以前部署的手机基站进行建设覆盖
D．增强 AP 功率

试题（63）分析

本题考查 WLAN 网络建设的相关优化知识。

根据题目要求，新建自己的 WLAN 无线网络投资大，而且可能与现有无线网的 AP 形成干扰。利用以前部署的手机基站进行建设覆盖其覆盖范围、速率等不能保证。增强 AP 功率不能满足网络接入的需求。利用学校现有无线网络，在 AP 上增加一个自己的 SSID 可以很方便地实现网络接入的需求同时又节省了投资，可以说是最合理的方案。

参考答案

（63）B

试题（64）

某学校建有宿舍网络，每个宿舍有 4 个网络端口，某学生误将一根网线接到宿舍的两个网络接口上，导致本层网络速度极慢几乎无法正常使用，为避免此类情况再次出现，管理员应该____（64）____。

（64）A．启动接入交换机的 STP 协议　　B．更换接入交换机
C．修改路由器配置　　D．启动交换机的 PPPoE 协议

试题（64）分析

本题考查网络故障排查的相关知识。

根据题意，将一根网线接到宿舍的两个网络接口上，很明显是形成了环路。网络环路会带来广播风暴、多重复数据帧、MAC 地址表不稳定等因素，解决方法就是利用生成树协议 STP。该协议可使用环路网络，解决必需的算法完成途径冗余，同时将环路修剪成无环路的树型网络，从而防止报文在环路网络中无限循环。本题中的其他方法都不能解决网络环路问题。

参考答案

（64）A

试题（65）

互联网上的各种应用对网络指标的敏感性不一，下列应用中对延迟抖动最为敏感的是____（65）____。

（65）A．浏览页面　　B．视频会议　　C．邮件接收　　D．文件传输

试题（65）分析

本题考查互联网上的应用对网络指标的敏感性。

实时视频的传输对带宽、延迟、延迟抖动和丢包率有较高的要求。而其中网络出现

延迟、抖动，将会给视频会议带来声画不同步，严重影响会议质量。而对浏览网页、接收邮件以及文件传输影响不大。

参考答案

（65）B

试题（66）

有 3 台网管交换机分别安装在办公楼的 1-3 层，财务部门在每层都有 3 台电脑连接在该层的一个交换机上。为了提高财务部门的安全性并容易管理，最快捷的解决方法是<u>（66）</u>。

（66）A．把 9 台电脑全部移动到同一层然后接入该层的交换机
B．使用路由器并通过 ACL 控制财务部门各主机间的数据通信
C．为财务部门构建一个 VPN，财务部门的 9 台电脑通过 VPN 通信
D．将财务部门 9 台电脑连接的交换机端口都划分到同一个 VLAN 中

试题（66）分析

本题考查网络管理维护的相关知识。

根据题意，A 选项需要变动财务部门的电脑，变换办公室要改变办公流程比较麻烦；B 选项要增加路由器，成本较高；C 选项需要搭建 VPN，配置以及管理成本复杂；综合来看，D 选项最快捷、成本最低。

参考答案

（66）D

试题（67）

在诊断光纤故障的仪表中，设备<u>（67）</u>可在光纤的一端就测得光纤的损耗。

（67）A．光功率计　　B．稳定光源
C．电磁辐射测试笔　　D．光时域反射仪

试题（67）分析

本题考查网络测试仪器的相关知识。

光功率计是指用于测量绝对光功率或通过一段光纤的光功率相对损耗的仪器。稳定光源是对光系统发射已知功率和波长的光。稳定光源与光功率计结合在一起，则能够测量光纤系统连接损耗、检验连续性，并帮助评估光纤链路传输质量。

光时域反射仪（OTDR）是通过对测量曲线的分析，了解光纤的均匀性、缺陷、断裂、接头耦合等若干性能的仪器。它根据光的后向散射与菲涅耳反向原理制作，利用光在光纤中传播时产生的后向散射光来获取衰减的信息，可用于测量光纤衰减、接头损耗、光纤故障点定位以及了解光纤沿长度的损耗分布情况等，是光缆施工、维护及监测中必不可少的工具。在诊断光纤故障的仪表中 OTDR 是最经典的也是最昂贵的仪表。与光功率计和光万用表的两端测试不同 OTDR 仅通过光纤的一端就可测得光纤损耗。

电磁辐射测试笔主要功能是检测出您周围的电磁辐射源。

参考答案

（67）D

试题（68）

某公司采用 ADSL 接入 Internet，开通一段时间来一直都比较正常，近一周经常出现间歇性的速度变慢，拔掉 Modem 的直流电源线，信号正常。更换一个新 Modem 及其直流电源适配器，仍然是呈现网速随机波动。导致该 ADSL 间歇性速度变慢的可能原因是<u>（68）</u>。

（68）A．电话线路过长　　B．电话线腐蚀老化
C．有强信号干扰源　　D．网卡质量不稳定

试题（68）分析

本题考查网络维护的相关知识。

根据题意，电话线路过长不会在开通的一段时间都正常，拔掉 Modem 的直流电源信号就正常，说明不是电话线路腐蚀老化和网卡质量不稳定。而更换一个新 Modem 及其直流电源适配器，仍然是呈现网速随机波动，说明不是电源的问题，只能是周边突然产生了强的信号干扰源。

参考答案

（68）C

试题（69）

在光缆施工中，应该特别注意光缆的弯曲半径问题，以下说法中不正确的是<u>（69）</u>。

（69）A．光缆弯曲半径太小易折断光纤
B．光缆弯曲半径太小易发生光信号的泄露影响光信号的传输质量
C．施工完毕光缆余长的盘线半径应大于光缆半径的 15 倍以上
D．施工中光缆的弯折角度可以小于 90 度

试题（69）分析

本题考查光缆施工中的注意事项。

在光缆施工中，要特别注意转弯时光缆弯折角度尽量别超过 90 度，否则容易折断。光缆的弯曲半径弧度不能太小，弧度太小易折断光纤，同时易造成折射损耗过大导致色散现象，也就是容易发生光信号的泄露影响光信号的传输质量。施工完毕光缆余长的盘线半径应大于光缆半径的 10～15 倍以上。

参考答案

（69）D

试题（70）

为满足企业互联业务需求，某企业在甲地的 A 分支机构与在乙地的企业中心（甲乙两地相距 50km），通过租用一对 ISP 的裸光纤实现互联，随着企业业务的扩大，要使得

甲地的另外 B、C、D 三个分支机构也能接入到企业中心，所采用的比较快捷和经济的做法是＿＿（70）＿＿。

（70）A．使用 CWDM 设备　　B．租用多对 ISP 的裸光纤
C．租用多条 DDN 专线　　D．使用 DWDM 设备

试题（70）分析

本题考查光纤传输中波分复用设备的相关知识。

把不同波长的光信号复用到一根光纤中进行传送的方式统称为波分复用（WDM）方式，这种技术利用了一根光纤可以同时传输多个不同波长的光载波的特点，把光纤可能应用的波长范围划分成若干个波段，每个波段用作一个独立的通道传输一种预定波长的光信号。通信系统的设计不同，每个波长之间的间隔宽度也有差别，按照通道间隔差异，WDM 可以细分为 CWDM、DWDM 等。而 CWDM 的成本比 DWDM 的成本要少 50%以上。根据题意，租用裸光纤和 DDN 专线都不是经济快捷的方式，所以选项为 A。

参考答案

（70）A

试题（71）～（75）

BGP is an inter-autonomous system routing protocol; it is designed to be used between multiple autonomous ＿（71）＿. BGP assumes that routing within an autonomous system is done by an intra-autonomous system routing protocol. BGP does not make any assumptions about intra-autonomous system ＿（72）＿ protocols employed by the various autonomous systems. Specifically, BGP does not require all autonomous systems to run the same intra-autonomous system routing protocol.

BGP is a real inter-autonomous system routing protocol. It imposes no constraints on the underlying Internet topology. The information exchanged via BGP is sufficient to construct a graph of autonomous systems connectivity from which routing loops may be pruned and some routing ＿（73）＿decisions at the autonomous system level may be enforced.

The key feature of the protocol is the notion of Path Attributes. This feature provides BGP with flexibility and expandability. Path ＿（74）＿ are partitioned into well-known and optional. The provision for optional attributes allows experimentation that may involve a group of BGP ＿（75）＿ without affecting the rest of the Internet. New optional attributes can be added to the protocol in much the same fashion as new options are added to the Telnet protocol, for instance.

（71）A．routers　B．systems　C．computers　D．sources
（72）A．routing　B．switching　C．transmitting　D．receiving
（73）A．connection　B．policy　C．source　D．consideration
（74）A．states　B．searches　C．attributes　D．researches
（75）A．routers　B．states　C．meters　D．costs

参考译文

BGP 是自治系统间的路由协议，它被应用于多个自治系统之间。BGP 假定，自治系统内部的路由已经由自治系统内部的路由协议搞定。BGP 对于各个自治系统采用的自治系统内部路由协议没有任何假定的条件。特别，也不要求所有的自治系统都运行同样的自治系统内部路由协议。

BGP 是一个实用的自治系统间的路由协议。它对底层的 Internet 技术没有任何限制。通过 BGP 交换的路由信息足以构造一个自治系统连接图，据此对路由环路进行修剪，并在自治系统这一级实施路由策略决策。

这个协议关键的特点是通路属性的表示。这个特点为 BGP 提供了灵活性和可扩展性。通路属性被划分为众所周知的和任选的两类。提供的任选属性可以在一组 BGP 路由器中进行实验而不影响因特网的其余部分。新的任选属性可以被加入到协议中，这种方式就像是新的选项被加入到 Telnet 协议中一样。

参考答案

（71）B （72）A （73）B （74）C （75）A

第 14 章　2012 下半年网络规划设计师下午试卷 I 试题分析与解答

试题一（共 25 分）

阅读以下关于某大学校园网的叙述，回答问题 1 至问题 4。

某大学校园网经过多年的建设已初具规模，由于校内相关的科研单位有接入到以 IPv6 为核心的下一代互联网中进行相关研究的需求，同时为了积极探索解决学校公网 IPv4 地址的短缺、现有网络安全等方面的问题，学校网络中心计划对现有校园网进行 IPv6 技术升级。学校现有的网络拓扑如图 1-1 所示。

（1）接入层：完成 IPv4 用户接入，设备是二层接入交换机/三层接入交换机。

（2）汇聚层：完成接入用户的汇聚，汇聚交换机是盒式或机架式三层交换机，目前不支持 IPv6 业务。

（3）核心层：是整个网络的核心（机架式三层交换机，目前不支持 IPv6 业务），同时连接外部网络的出口，是整个园区网业务流量通往 IPv4 主干网或者 IPv6 主干网的必经之路。

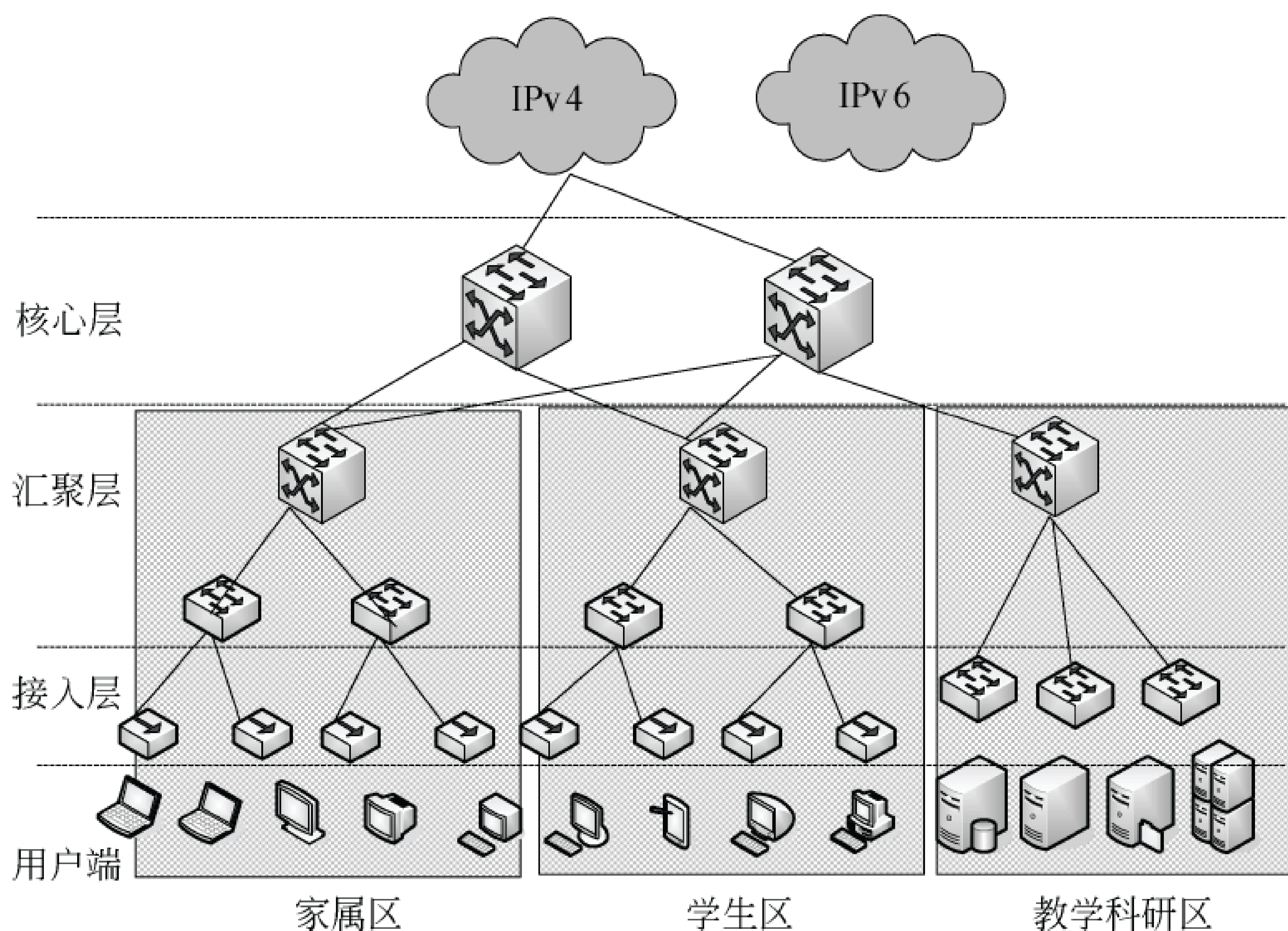


图 1-1

【问题 1】（5 分）

为了实现 IPv4 网络向 IPv6 网络的过渡和转换，IETF 制订的解决过渡问题的基本技

术方案有三种。在进行 IPv6 升级的初期，由于教学科研区访问 IPv6 网络的需求比较迫切，学校希望花费较少的资金就能使教学科研区访问 IPv6 网络上的相关资源，简述三种技术方案的要点，并依据需求进行过渡技术方案选择。

【问题 2】（8 分）

随着网络建设的不断升级，为把校园网积极推进到以 IPv6 为核心的下一代互联网中，要求学生区和教学科研区的 IPv6 用户能够访问 IPv6 网络资源，同时实现这两个区域之间 IPv6 资源的互访。

（1）基于上述的需求，对过渡方案进行了调整，网络结构如图 1-2 所示，请在尽量节省资金的情况下给出该校园网 IPv6 技术升级的过渡方案，并进行设备升级和网络调优（网络设备调整等）的方案设计。

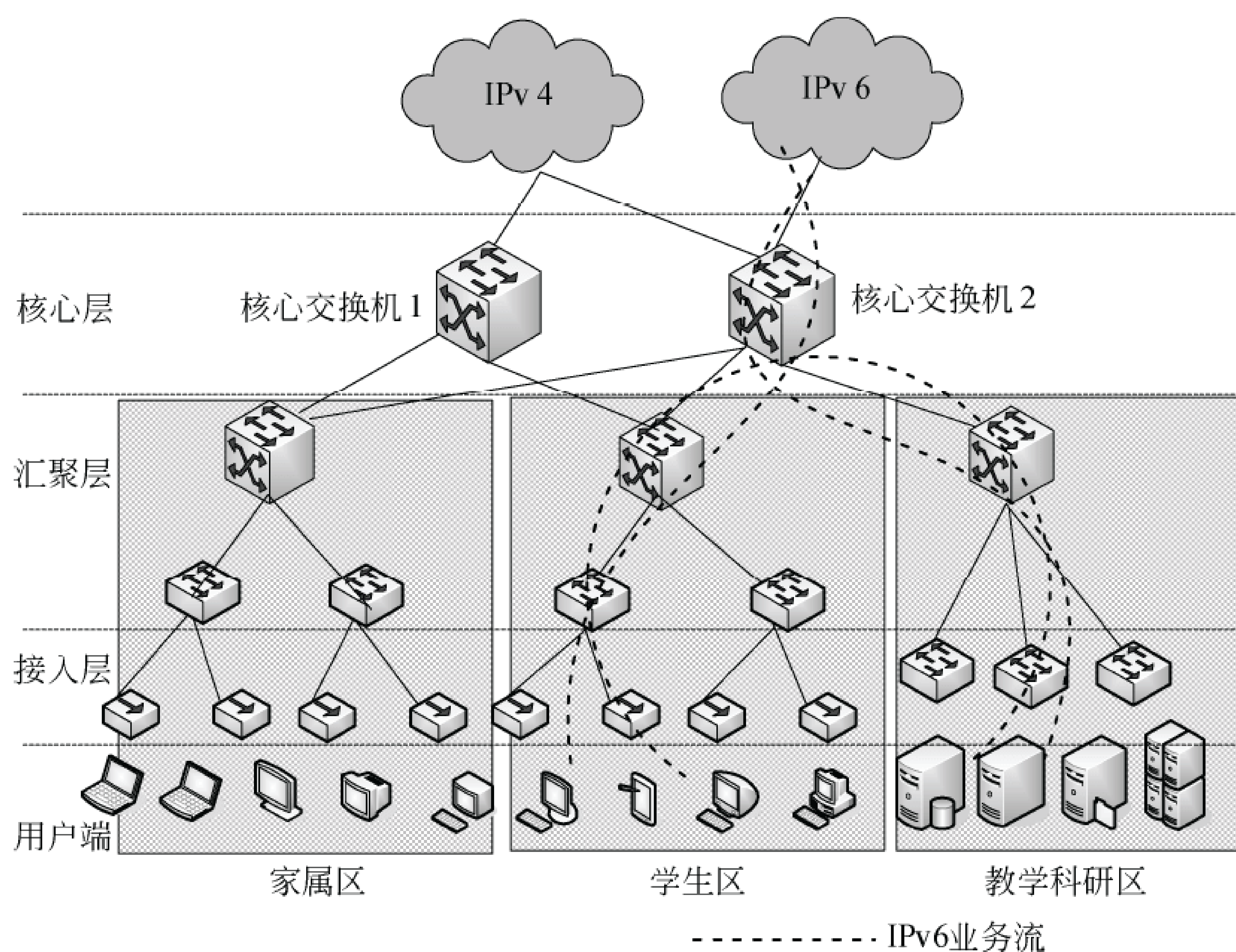


图 1-2

（2）因家属区个别用户也想接入到 IPv6 网络中访问相关资源，现在核心交换机 2 上开启 ISATAP 隧道，隧道服务器地址为 isatap.xuexiao.edu.cn。

若家属区客户机为 win xp(sp1 及以上)，完成下面的步骤，使得客户机能够通过 ISATAP 隧道接入 IPv6 网络。

C:>______①______//安装 IPv6 协议

C:>______②______//设置隧道终点

【问题 3】（8 分）

NDP（Neighbor Discovery Protocol，邻居发现协议）是 IPv6 的一个关键协议，它组

合了 IPv4 中的 ARP、ICMP路由器发现和 ICMP 重定向等协议，并对它们做了改进，作为 IPv6 的基础性协议，NDP 还提供了前缀发现、邻居不可达检测、重复地址监测、地址自动配置等功能。进行 IP 地址规划及路由方案设计，包括：

（1）在现阶段网络的 IPv6 技术升级中，IPv6 地址分配的两种分配机制是什么？

（2）在本方案中服务器端和用户端分别采用的 IPv6 地址分配机制是什么？

（3）在 IPv4 的网络中，校园网内部路由协议采用 OSPF，在 IPv6 的网络中采用的路由协议是什么？

（4）接入到 IPv6 网络中的边界路由器采用何种接入方式。

【问题 4】（4 分）

近年来国家大力推进 IPv4 向 IPv6 的过渡，但是基于 IPv6 的网络部署还不能达到国家的战略要求。

（1）你认为影响 IPv6 发展的因素主要有哪些。

（2）对于学校现有 IPv6 网络的运维的建议。

试题一分析

本题考查 IPv4 向 IPv6 过渡、IPv6 网络的相关配置规划以及 IPv6 网络的发展等内容。

【问题 1】

为了适应大众的需要，网络业务逐步呈现出宽带化、综合化、多样化和个性化的特点，IPv4 向 IPv6 网络过渡已是大势所趋。基于 IPv6 的下一代互联网技术的迅速发展，为网络发展提供了更为有利的扩展空间，然而受到诸多条件的限制，想要很快完成从 IPv4 到 IPv6 网络的转换是不切实际的。

目前已有多种策略和技术方案及其实现可以完成从 IPv4 向 IPv6 的转换，但都仍有局限性。按工作原理划分有以下三种：隧道技术、双协议栈技术和协议翻译技术。

（1）隧道技术

隧道技术：隧道技术的工作原理是在 IPv6 网络与 IPy4 网络间的隧道入口处，路由器将 IPv6 的数据分组封装入 lPv4 中。IPv4 分组的源地址和目的地址分别是隧道入口和出口的 IPv4 地址，在隧道的出口处再将 IPv6 分组取出转发给目的节点。换句话说，就是通过 IPv4 网络实现“IPv6 孤岛”之间的互通。

这种技术能充分利用现有的网络资源，但是没有解决 IPv4 和 IPv6 网络之间的互通，因此只能是是过渡初期较为方便的选择。

（2）双协议栈技术

双栈协议技术指在完全过渡到 IPv6 之前，使一部分主机或路由器同时支持 IPv4 和 IPv6 两种协议，这样双协议栈设备既能识别 IPv4 报文也能识别 IPv6 报文，从而实现与 IPv4 和 IPv6 网络的数据通信。主机具体使用 IPv4 协议还是 IPv6 协议来发送和接收数据包是由目的地址来决定的。

这种机制主要用来解决纯 IPv6 网络中的双栈主机与其他 IPv4 节点通信的问题，但没有解决 IPv4 地址的问题。

（3）协议翻译技术

翻译技术实际是一种协议转换技术，即为了使 IPv4 和 IPv6 网络中的主机能相互识别对方而进行的协议头之间的转换。其中 NAT-PT 是实现翻译策略的一种主要技术。翻译转换技术的优点是不需要进行 IPv4、IPv6 节点的改造就能有效解决 IPv4 节点与 IPv6 节点相互通信的问题，根据 NAT-PT 原理，过渡初期“IPv6 孤岛”中的主机通过转换设备，将其 IPv6 地址转换成合法的 IPv4 地址进而访问 IPv4 的网络。

以上是目前存在的一些由 IPv4 网络过渡到 IPv6 的机制, 无论采取哪一种机制，对 DNS 的扩展都是必须的。这些过渡机制仍不是普遍适用的，常常需要和其他技术组合使用。在实际应用时需要综合考虑各种实际情况来制定合适的过渡策略。表 1 给出三种不同技术的过渡方案对比。

表 1　采用三种不同技术的过渡方案对比

过渡技术名称	优　　点	缺　　点	使 用 场 合
隧道技术	以现有 IPv4 网络传递 IPv6 数据，无须大量 IPv6 路由和专用链路，是过渡阶段最容易采用的技术	需避免路由回环和路由泄露，不能解决 IPv4 和 IPv6 网络的互联互通	连接到纯 IPv4 网络上的 IPv6 孤岛之间通信
双栈技术	同时运行 IPv4 和 IPv6 两套协议栈，完全兼容 IPv4 和 IPv6	没有解决 IPv4 地址耗尽的问题	任何 IPv4/IPv6 网络
翻译技术	在通信中间设备完成 IPv4 和 IPv6 网络之间地址转换和协议翻译，分组路由对端节点透明	IPv4 节点访问 IPv6 节点的方法复杂，网络设备开销大，一般在其他互通方式实现不了的情况下使用	IPv6 孤岛与 IPv4 海洋之间的通信

校园网络过渡的实质是将目前的 IPv4 网络全面向 IPv6 网络过渡。为了更充分地利用。校园网现有的网络设备，降低升级成本，从而实现平滑稳定地向 IPv6 过渡的目标，过渡的具体实施可分为四个阶段进行：

第一阶段，可根据个别用户或者部门的需求，建立起若干 IPv6 网络。这些 IPv6 网络即所谓的“IPv6 孤岛”。这些“IPv6 孤岛”通过隧道技术与学校的实验网进行联通，并经此连接到 IPv6 网络中。显然这时 IPv4 网络是占主导地位的。通过路由器访问外部 IPv6 接入主机必须是双栈主机，并通过配置隧道先连接到网络中心的 IPv6 路由器，从而访问外部 IPv6。

第二阶段，越来越多的“IPv6 孤岛”逐渐变大、变多，数量与 IPv4 网络相当，与 IPv4 网络通讯增加，IPv6 网络规划越来越规范，此时可综合采用双协议栈技术和动态 NAT-PT 技术，这就需要对核心层和汇聚层的设备进行升级。为保证核心层设备性能，

同时尽量减少对原网络线路的改动，建议直接将核心层设备升级为支持双协议栈技术的设备。

这个阶段 IPv4 和 IPv6 网同时存在且数量相当，因此需要解决各种网络中各种主机的通信问题。内部 IPv4 主机之间、IPv6 主机之间的数据通信没有问题，IPv6 网络和 IPv4 网络通过 NAT-PT 技术实现相互通信。IPv4 网络仍然通过原核心交换与外部 IPv4 网络联通，IPv6 网络则通过网络中心的核心设备与外部 IPv6 网络通信。

第三阶段，IPv6 将占主导地位，IPv4 网络逐渐变为“孤岛”。这个阶段与 IPv6 发展的第一个阶段非常相似，所以此时也可采用隧道技术进行部署，与第一阶段不同的是此时互联的是 IPv4 网络。

第四阶段，经过设备的更新换代，网络中所有设备都已支持 IPv6，IPv4 网络逐渐被 IPv6 所替代，直至 IPv4 网络节点完全被淘汰，此时校园网完全升级为纯 IPv6 网络，各网络节点间也都采用基于 IPv6 的通信方式。

【问题 2】

根据题目要求，目前校园网已经发展到 IPv4 与 IPv6 的共存期。

全双栈模式适合在新建的校园网或原有网络不断更新发展到中期时使用。全双栈模式要求核心层和汇聚层选用双栈交换机，接入层可使用现有的二层交换机，其中汇聚层也可采用双栈路由设备。对于双栈终端，IPv4 网关和 IPv6 网关均部署在汇聚双栈三层交换机上。IPv4 和 IPv6 协议可以同时运行，使用协议翻译机制让纯 IPv4 节点和 IPv6 节点进行通信。全双栈模式提供的 IPv6 接入服务范围广，可获得较大规模 IPv6 建设和使用经验。不必为不同类型的用户单独部署网络配置，开销小，方便管理，IPv4 和 IPv6 的逻辑界面清晰。

针对网络拓扑结构，可考虑购买或者升级学生区和教学科研区的核心和汇聚交换机，支持 IPv6，接入层网络设备暂时不用调整。同时为保护投资，如果学生区和教学科研区有淘汰下来的网络设备也可用在家属区的网络维护中。

ISATAP 的全名是 Intra-Site Automatic Tunnel Addressing Protocol，它将 IPv4 地址加入 IPv6 地址中，当两台 ISATAP 主机通讯时，可自动抽取出 IPv4 地址建立 Tunnel 即可通讯，且并不需透过其他特殊网络设备，只要彼此间 IPv4 网络通畅即可。

通过 ISATAP 隧道接入 IPv6 环境的方法

学校 ISATAP 隧道路由器的 IPv4 地址是：isatap.xuexiao.edu.cn

用户设置 ISATAP 隧道的接入点为：isatap.xuexiao.edu.cn

Windows XP/2003 下配置方法

进入命令提示符

```
C:\>netsh
netsh>int
netsh interface>IPv6
```

netsh interface>IPv6>install //安装 IPv6 协议

netsh interface IPv6>ISATAP

netsh interface IPv6 ISATAP>set router isatap.xuexiao.edu.cn //设置隧道终点

此后，通过 ipconfig 应该可以看到一个本校前缀的 v6 地址，hostid 为 0:5efe:a.b.c.d，其中 a.b.c.d 为你的真实的 IPV4 地址，这样即可访问 IPv6 资源。

【问题 3】

IPv6 地址是独立接口的标识符，所有的 IPv6 地址都被分配到接口，而非节点。由于每个接口都属于某个特定节点，因此节点的任意一个接口地址都可用来标识一个节点。IPv6 有三种类型地址：

（1）单点传送（单播）地址

一个 IPv6 单点传送地址与单个接口相关联。发给单播地址的包传送到由该地址标识的单接口上。但是为了满足负载平衡系统，在 RFC 2373 中允许多个接口使用同一地址，只要在实现中这些接口看起来形同一个接口。

（2）多点传送（组播）地址

一个多点传送地址标识多个接口。发给组播地址的包传送到该地址标识的所有接口上。IPv6 协议不再定义广播地址，其功能可由组播地址替代。

（3）任意点传送（任播）地址

任意点传送地址标识一组接口（通常属于不同的节点），发送给任播地址的包传送到该地址标识的一组接口中根据路由算法度量距离为最近的一个接口。如果说多点传送地址适用于 one-to-many 的通讯场合，接收方为多个接口的话，那么任意点传送地址则适用于 one-to-one-of-many 的通讯场合，接收方是一组接口中的任意一个。

IPv6 地址为 128 位，如果手工设置要花费很多时间。IPv6 协议可以手工静态输入，也支持地址自动配置，地址自动配置是一种即插即用的机制。IPv6 节点通过地址自动配置得到 IPv6 地址和网关地址。

IPv6 支持无状态地址自动配置和状态地址自动配置两种地址自动配置方式。在无状态地址自动配置方式下，需要配置地址的网络接口先使用邻居发现机制获得一个链路本地地址。网络接口得到这个链路本地地址之后，再接收路由器宣告的地址前缀，结合接口标识得到一个全球地址。而状态地址自动配置的方式，如动态主机配置协议（DHCP），需要一个 DHCP 服务器，通过客户机/服务器模式从 DHCP 服务器处得到地址配置的信息。

在本次升级方案中，用户端数量众多，而且 IPv6 地址长达 128 位，可采用无状态地址自动分配机制来自动分配地址，服务器端因为数量较少且固定，同时要在域名系统中配置可考虑采用静态手工配置方式。

校园网内部路由协议采用 OSPF 动态路由协议，IPv6 路由协议可采用 OSPFv3 动态路由。这样在地址规划、区域设计上就具有很大的便利性。

在出口路由方面，因为目前 IPv6 的出口只有一个，所以考虑采用静态路由的方式。

【问题 4】

IPv4 向 IPv6 过渡主要包含以下几个方面的过渡：

（1）网络的过渡

为了支持 IPv6 协议，主要有两种方式可以选择：一是用软件升级现有的 IPv4 路由设备，使它能够运行 IPv6 协议；另一种方法是购买新的支持 IPv6 协议的路由设备，并采用相应的链路资源，这样使它们在物理上构成两个独立的网络环境。网络的过渡包括网络节点的过渡、网络设备的过渡、网关的过渡。

（2）客户端的过渡

过渡到 IPv6 协议需要升级用户的终端设备，它包括客户端的网络协议和应用程序的升级。

（3）应用程序的过渡

由于 IPv6 协议的应用程序不及 IPv4 协议的应用程序那般普及，所以开发的应用程序对于低层协议应是透明的，即 IPv4 协议下能使用，IPv6 协议下也能使用。另外，将来 IPv6 在得到普遍支持后，用户还可以继续使用原来的纯 IPv4 应用程序。

（4）IPv4/IPv6 网络互通

校园网络正面临从传统 IPv4 到 IPv6 的过渡以及一段时期的共存。如果主机不支持双栈，那么就必然存在纯 IPv4 和纯 IPv6 节点之间的互通问题，这也是过渡时期必须面对的主要问题之一。使用网络地址翻译/协议翻译(NAT-PT)转换技术能较好地解决该问题，但它在支持数据的透明性方面存在一定的问题。校园网络的过渡各个环节紧密相扣，相辅相成。网络的过渡脱离了客户端的过渡、应用程序的过渡及 IPv4/IPv6 的网络互通，网络的过渡就无法进行。因此，这四个方面的演进必须同时进行。

IPv4 向 IPv6 过渡是一个复杂的、系统的社会工程，超越了简单的技术范畴，也超出了各大运营商的职责范畴，需要产业链协同推动。IPv4 向 IPv6 过渡有其内在的规律，我们只有在认识规律并遵循规律的基础上，顺势而为，才能获得成功。这个规律就是过渡需要经历 IPv4 资产保值、IPv6 准备和 IPv6 繁荣这三个演进阶段，我们只能在有限范围内缩短或者延长某一阶段的时间，但是无法颠倒顺序。不同阶段的场景和任务不同，所依赖的技术也不同，所以不同的技术将先后登场，是一场技术的接力赛。中间过渡技术在完成使命后，最后全部退出舞台，只留下 IPv6 造福人类。在向 IPv6 过渡期间，重点和难点在接入网络部分，其次是互联互通部分，骨干网络基本具备。当然，在过渡过程中，基于 IPv6 的应用资源还是较少，这中间最关键的因素可能是缺少杀手级的应用来推动。

校园网 IPv6 技术升级中的网络部分改造虽然可以很快完成，但相关的支撑系统的建设和应用系统的迁移才刚刚开始，需要继续完善校园网网络管理与安全监控系统、接入和计费等，使其成为学校新一代先进的教学和科研信息基础设施。同时，如何建设一个

安全的下一代互联网是一个全新的课题。要想将下一代互联网建设到目前 IPv4 网络的阶段，还有比较长的一段路要走。在这些方面，有实力的学校可以进行有益的探索，进行自主科研开发，也可以通过和厂商合作进行共同开发，如果有成熟的产品也可进行推广应用。

参考答案

【问题 1】

简述三种技术要点：

隧道技术，以现有 IPv4 网络传递 IPv6 数据，无须大量 IPv6 路由和专用链路，是过渡阶段最容易采用的技术，一般用来进行纯 IPv4 网络上的 IPv6 孤岛之间通信。

双栈技术，同时运行 IPv4 和 IPv6 两套协议栈，完全兼容 IPv4 和 IPv6。

翻译技术，在通信中间设备完成 IPv4 和 IPv6 网络之间地址转换和协议翻译，分组路由对端节点透明。IPv4 节点访问 IPv6 节点的方法复杂，网络设备开销大，一般在其他互通方式实现不了的情况下使用。

要求在实现教学科研区访问 IPv6 网络上的相关资源功能的基础上费用花费最小，网络结构不变且部署方便，可在核心设备上采用隧道接入技术实现其功能。

【问题 2】

（1）实现的技术方案选择双栈模式。

设备升级模式为：新建（升级）学生区和教学科研区的核心和汇聚交换机，支持 IPv6。

网络调优方案：将学生区和教学科研区的核心、汇聚交换机以及其他不能进行 IPv6 升级的设备调整到家属区的网络，以满足家属区网络的运维需求。

（2）① netsh interface ipv6 install 或者 ipv6 install

② netsh interface ipv6 isatap set router isatap.xuexiao.edu.cn

【问题 3】

（1）两种，无状态地址自动分配机制，状态地址自动分配机制。

（2）用户端采用无状态地址自动分配机制，服务器端采用静态手工配置方式。

（3）采用 OSPFv3，实现与 IPv4 网络的隔离与统一。

（4）边界路由器对外出口只有一个，采用静态路由方式接入。

【问题 4】

（1）当前影响 IPv6 发展的因素主要有软硬件设备的升级；IPv6 网络资源不足，应用缺乏；v4/v6 的透明过渡/无缝连接技术问题；运营商的需求不大等问题，其中最关键的应该是缺少杀手级的应用。

（2）目前大多数网管产品还不支持 IPv6 下的管理功能，计费认证功能等也亟待开发，因此现阶段的运维技术实力较强的学校可采用利用开源产品自主开发，技术实力一般的学校采用与厂商合作开发的方式。

试题二（共 25 分）

阅读以下关于某国有大型煤化集团数据中心的叙述，回答问题 1 至问题 4。

近年来，云计算技术的蓬勃发展为整个 IT 行业带来了巨大变革。传统数据中心已经难以满足新形势下日益增长的高性能及高性价比需求，并且无法支持云环境下更加灵活的按带宽租赁数据中心网络的运营方式。该集团随着信息系统业务的不断扩展上线，对高密度服务器及高度自动化管理系统的需求不断增长，建设云数据中心的需求应运而生。

【问题 1】（7 分）

如图 2-1 所示，依据集团总部业务应用的需求，集团数据中心网络按功能将划分为七大区：核心交换区、核心业务区、办公区、互联网接入区、运维管理区、广域网接入区、外联业务区。二级板块及其下属子分公司可参考建立符合自身情况的局域网络。

你认为这七大区域应该如何分布，请根据图 2-1 所示填写图中（1）～（7）区域名称。

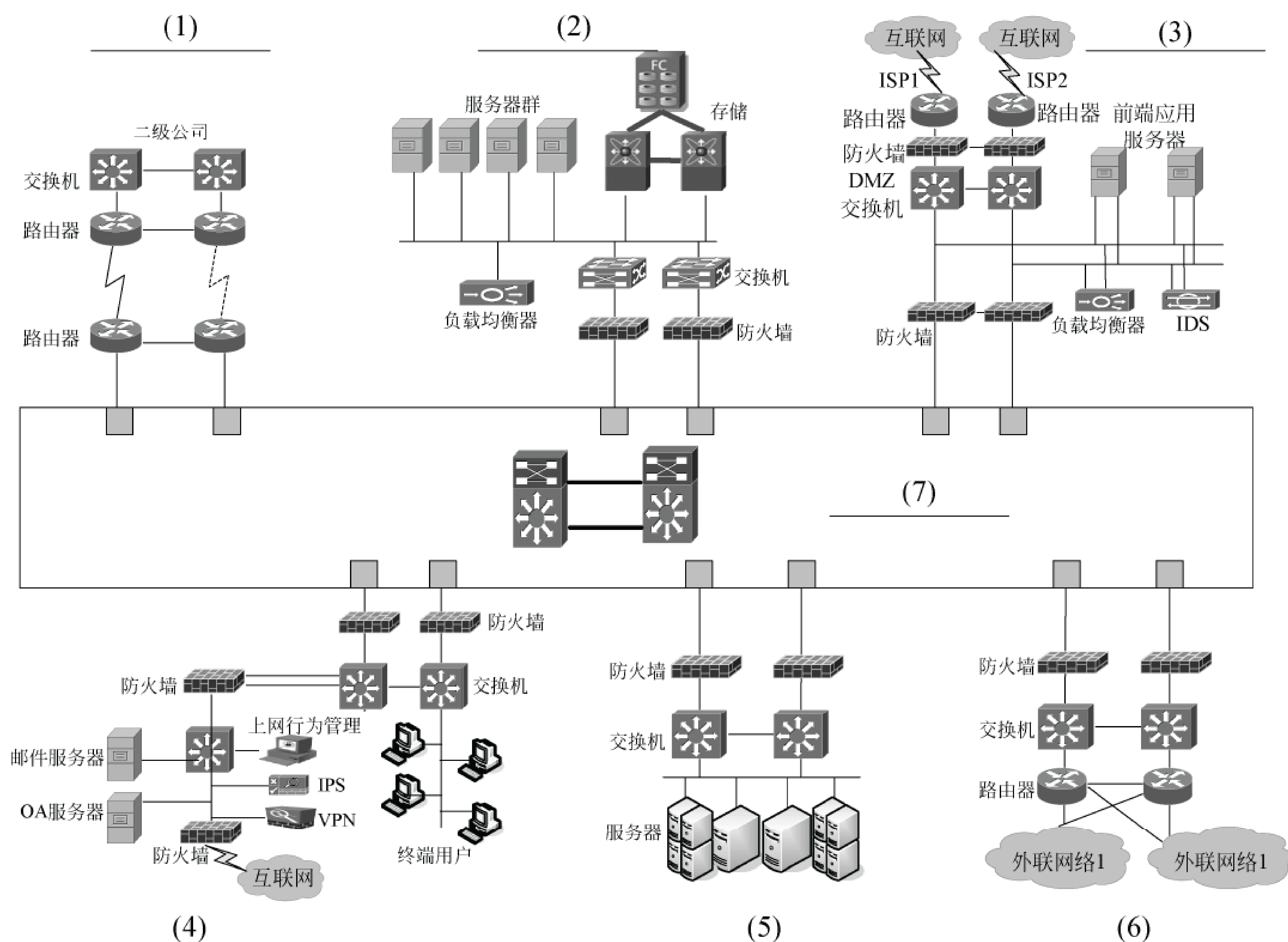


图 2-1

【问题 2】（6 分）

云数据中心是指以客户为中心、以服务为导向，基于高效、低能耗的 IT 与网络基础

架构，利用云计算技术，自动化地按需提供各类云计算服务的新一代数据中心。云数据中心是传统数据中心的升级，是新一代数据中心的演进方向。

（1）请简述云数据中心的特点。

（2）云计算的关键技术有虚拟化技术、分布式计算技术、安全与隐私保护技术等，请简要说明云数据中心在 IT 基础设施虚拟化技术方面主要包括哪些技术。

【问题 3】（6 分）

为增强该集团业务应用系统、重要数据的可用性，抵御灾难发生时带来的风险，该集团按照国家要求需要建设两地三中心的容灾备份方案。两地三中心是指主数据中心、同城灾备及异地灾备中心。两地三中心机房为业务应用系统建设提供基础配套设施。请画图说明两地三中心的数据中心架构采用的网络互联拓扑方案，并给出理由。

【问题 4】（6 分）

该集团数据存储量巨大，生产数据、安全数据以及测试数据等需要进行频繁的快速读写，为保障这种应用的需求，该集团希望在数据中心的数据存储方式上既要保证存储的可扩展性还要保证数据的快速访问，同时对新服务器的部署也要考虑快速部署。

数据中心中数据采用的存储方式主要有 DAS、NAS、SAN 三种，请分别描述三种存储方式的原理，并根据集团要求设计在该集团的数据中心建设中应采用的存储方式，叙述采用这种方式的优点。

试题二分析

本题考查企业网络规划设计、云数据中心相关技术等内容。

【问题 1】

集团数据中心网络按功能将划分为七大区：核心交换区、核心业务区、办公区、互联网接入区、运维管理区、广域网接入区、外联业务区。其中各部分功能大致如下：

（1）核心交换区实现网络分区之间的通信流量路由、交换功能，是数据中心网络最核心的部分。核心交换区需要具备高可用、高性能架构，以来确保核心网络高可用及高效运行。

（2）核心业务区将提供核心业务应用系统的网络接入功能。核心业务区域集中了核心业务应用服务器和核心业务应用数据库服务器，为内部用户、内部业务人员提供应用服务的核心区域，需要采用较高可用性和更全面的安全防护措施。

（3）办公区包括两部分功能：一部分是办公用户网络接入提供内部员工办公电脑、移动等设备网络接入功能，满足企业内部员工访问内部业务应用系统；另一部分是用户互联网访问、办公邮件处理、内部文件传输等功能。

（4）互联网接入区提供互联网业务的接入访问网络，为保证网络安全需要部署外网防火墙，用于保护业务应用前端应用；部署内网防火墙，用于保护集团内部网络的安全；采用多条冗余的互联网链路，提高网络接入的可靠性。

（5）运维管理区提供运维管理系统（监控、信息化服务管理等）网络互联功能，运

维管理系统需与公司范围内的应用、基础设施通信，安全性要求较高。

（6）广域网接入区用于连接广域网络连接设备。

（7）外联业务区即企业边界网区域，具有如下特点：与外网互联，风险较大；与内网相连进行数据通信。

根据网络拓扑结构和各大区域网络功能划分可方便的区分各区域名称。

【问题 2】

云计算是一种将池化的集群计算能力通过互联网向内外部用户提供按需服务的互联网新业务，是传统 IT 领域和通信领域技术进步、需求推动和商业模式变化共同促进的结果，具有以网络为中心、以服务为提供方式、高扩展高可靠性、资源池化与透明化等 4 个特点，云计算的出现，使 IT 资源具备了可运营的条件。数据中心是云计算生态系统中的重要一环，在云计算模式下，信息的存储、处理、传递等功能均由网络侧完成，实际上由数据中心承担。由于传统数据中心存在资源利用率低、自动化程度低、能耗过高等一系列问题，无法有效承载云计算业务，因此基于云计算技术的新一代数据中心应运而生。

云数据中心是指以客户为中心、以服务为导向，基于高效、低能耗的 IT 与网络基础架构，利用云计算技术，自动化地按需提供各类云计算服务的新一代数据中心。云数据中心是传统数据中心的升级，是新一代数据中心的演进方向。云数据中心具有以下 5 个特点。

（1）资源池化

云数据中心内的 IT 资源和网络资源将构成统一的资源池，实现物理资源与逻辑资源的去耦合，用户仅需对逻辑资源进行相关操作而无需关注底层实际物理设备。

（2）高效智能

基于虚拟化、分布式计算等技术，利用低成本的集群设备实现高效廉价的信息承载、存储与处理，同时通过管理平台实现自动化的资源监控、部署与调度以及业务生命周期的智能管理。

（3）面向服务

整体架构以服务为导向，通过松耦合的方式实现多服务的综合承载与提供，云数据中心由提供资源变成提供服务，用户通过服务目录选择相关的服务，对底层实际资源透明。

（4）按需供给

底层基础架构在资源池化的基础上根据实际需求实现资源的动态伸缩，并提供完备的、细颗粒的计费功能，云数据中心还将根据上层应用的发展趋势，实现对底层物理设备的智能容量规划。

（5）绿色低碳

通过模块化的设计以及虚拟化等绿色节能技术，降低云数据中心的设备投入成本以

及运营维护成本，实现低 PUE 值的绿色低碳运营。

云计算的关键技术有虚拟化技术、分布式计算技术、安全与隐私保护技术等。

虚拟化技术是基础设施资源池建设的重要部分，虚拟化技术从软、硬件资源中抽象出来，提供不同颗粒度，功能相同的虚拟资源。虚拟化技术将增加软、硬件的复用，提升基础设施资源的利用率、灵活性及安全性、可用性。

基础设施虚拟化技术包括网络虚拟化、服务器虚拟化及存储虚拟化。

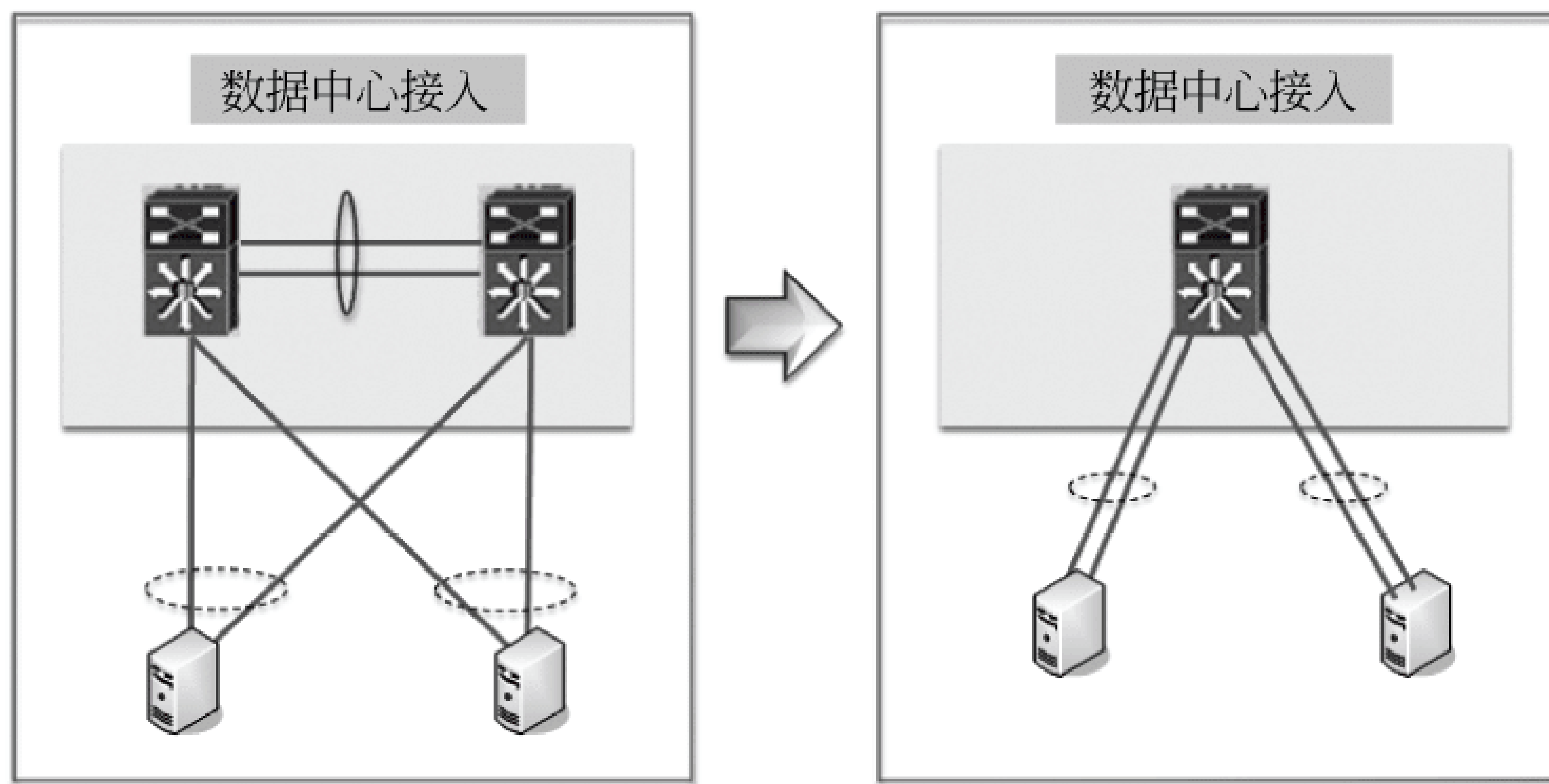
（1）网络虚拟化

相对于传统的物理网络资源，网络虚拟化能够带来的优点包括：虚拟网络资源带来了更好的灵活性及可扩展性；在不改变物理网络拓扑情况下，实现网络灵活配置满足信息系统的快速部署需求；通过共享的模式，最大限度地利用现有资源，降低成本。

常见的网络虚拟化包括：虚拟交换机、网络核心虚拟交换、虚拟防火墙等。

虚拟交换机包括基于软件或硬件设备虚拟交换机，单台交换机虚拟成多台虚拟交换机，实现虚拟服务器灵活的网络接入。主要提供虚拟服务器网络连接；实现对虚拟服务器网络配置策略的统一管理；实现物理刀片服务器的配置属性信息（网络及存储连接等）的集中管理，服务器的配置属性文件应用可加速失败服务器更换；实现虚拟服务器网络配置信息跨数据中心迁移。

网络核心虚拟交换技术去除了由生成树协议带来的网络资源空闲的状态，将两台交换机虚拟成为一台交换机，并作单一设备进行管理和使用，在网络中表现为一个网元节点；网络核心虚拟交换将简化网络架构、简化管理及配置，进一步增强冗余可靠性。实现负载均衡，提高网络设备性能。网络核心虚拟交换如下图所示。



虚拟防火墙将一台物理防火墙虚拟成若干相互独立、功能相同的虚拟防火墙。提供网络流量安全隔离功能，实现安全的虚拟网络环境。

（2）服务器虚拟化

服务器虚拟化的主要优点包括：提高服务器资源利用率，可减少能源消耗，降低基础设施总成本；提高运行在虚拟机上的应用系统的可用性；提高应用系统的安全性，实

现快速备份及恢复。当前主流的服务器虚拟化技术包括：X86 服务器虚拟化及 Unix 服务器虚拟化。

Unix 架构虚拟化技术包括分区技术及软件虚拟化技术，如下表所示。Unix 服务器架构的分区技术使操作系统能够直接访问到底层的物理资源，硬件分区技术支持的资源颗粒度较粗，例如最小单位是 1 颗 CPU；软件虚拟化技术的资源颗粒度较细，资源划分颗粒度较分区技术更小，资源调整更加灵活，例如最小单位是 0.1 颗 CPU。

技　术	特　性
硬件分区	具有硬件电气隔离功能； 分区的故障不影响其他分区，比如：HP　nPar
逻辑分区	在硬件层上抽象出虚拟化层，对资源进行组合而成的逻辑分区； 独占的硬件资源，但没有电气隔离，比如: HP vPar, IBM Lpar
软件虚拟化	在操作系统内，对特定应用分配计算资源

Unix 服务器架构虚拟化使用：测试、开发环境对资源的要求灵活，需要使用多种的虚拟化技术，如硬件、逻辑分区、软件虚拟化；生产环境采用硬件分区或逻辑分区技术。

X86 服务器虚拟化技术包括基于硬件的虚拟化技术和基于软件两种的虚拟化技术，如下表所示。

技　术	特　性
基于硬件的虚拟化技术	在硬件层上抽象出虚拟化层，对资源进行组合而成的逻辑分区； 具有较高的性能；稳定性好；分区之间安全隔离
基于软件的虚拟化技术	使用基于操作系统层之上的虚拟资源； 操作系统故障会影响所有虚拟机

X86 服务器虚拟化使用：X86 服务器虚拟化技术已比较成熟，并且硬件虚拟化的技术已成为主流；开发、测试环境选用不同厂商基于硬件的 X86 服务器虚拟化技术；生产环境采用基于硬件技术的 X86 服务器虚拟化技术，并选用成熟的、对 Windows 和 Linux 操作系统兼容的虚拟化技术，如 Microsoft Hyper-V、VMware 技术。

（3）存储虚拟化

存储虚拟化的优点包括：存储空间的统一分配，提高存储资源利用率；具有优异的灵活性及可扩展性；提供自动精简配置；自动数据迁移。

存储虚拟化主流技术包括基于主机的存储虚拟化，存储网络的虚拟化，以及基于存储设备的虚拟化，如下表所示。

存储虚拟化主流技术	特　点
基于主机存储的虚拟化	通过在主机系统中安装额外的设备驱动和软件来提供对物理磁盘的虚拟化功能，经过虚拟化的存储空间可以跨多个异构的磁盘阵列； 存储管理占用主机性能，管理比较复杂，每台主机都需要安装管理软件

续表

存储虚拟化主流技术	特　　点
基于存储网络的虚拟化	通过向存储网中（SAN）中添加虚拟引擎，实现对异构存储设备的虚拟化管理，根据数据流向分为带内虚拟化及带外虚拟化。 带内虚拟化：带内虚拟化是在主机与存储设备之间引入一层虚拟化引擎，所有数据及控制信息传输均通过该引擎；虚拟化引擎对所有通过的数据进行运算。 带外虚拟化：带外虚拟化是指虚拟化引擎处于数据传输路径之外，数据传输并不通过该引擎，带外虚拟化引擎仅向主机传送一些控制信息来完成物理设备和逻辑卷之间的地址映射。 存储网络的虚拟化不占用主机及存储资源，扩展性较好，技术比较成熟
基于存储设备的虚拟化	通过在存储控制器上添加虚拟化功能，实现存储磁盘的虚拟化管理；可以按需要对存储容量划分多个存储空间，实现多个主机系统的虚拟化管理；基于存储设备的虚拟化不占用主机及存储资源，扩展性较好，技术比较成熟

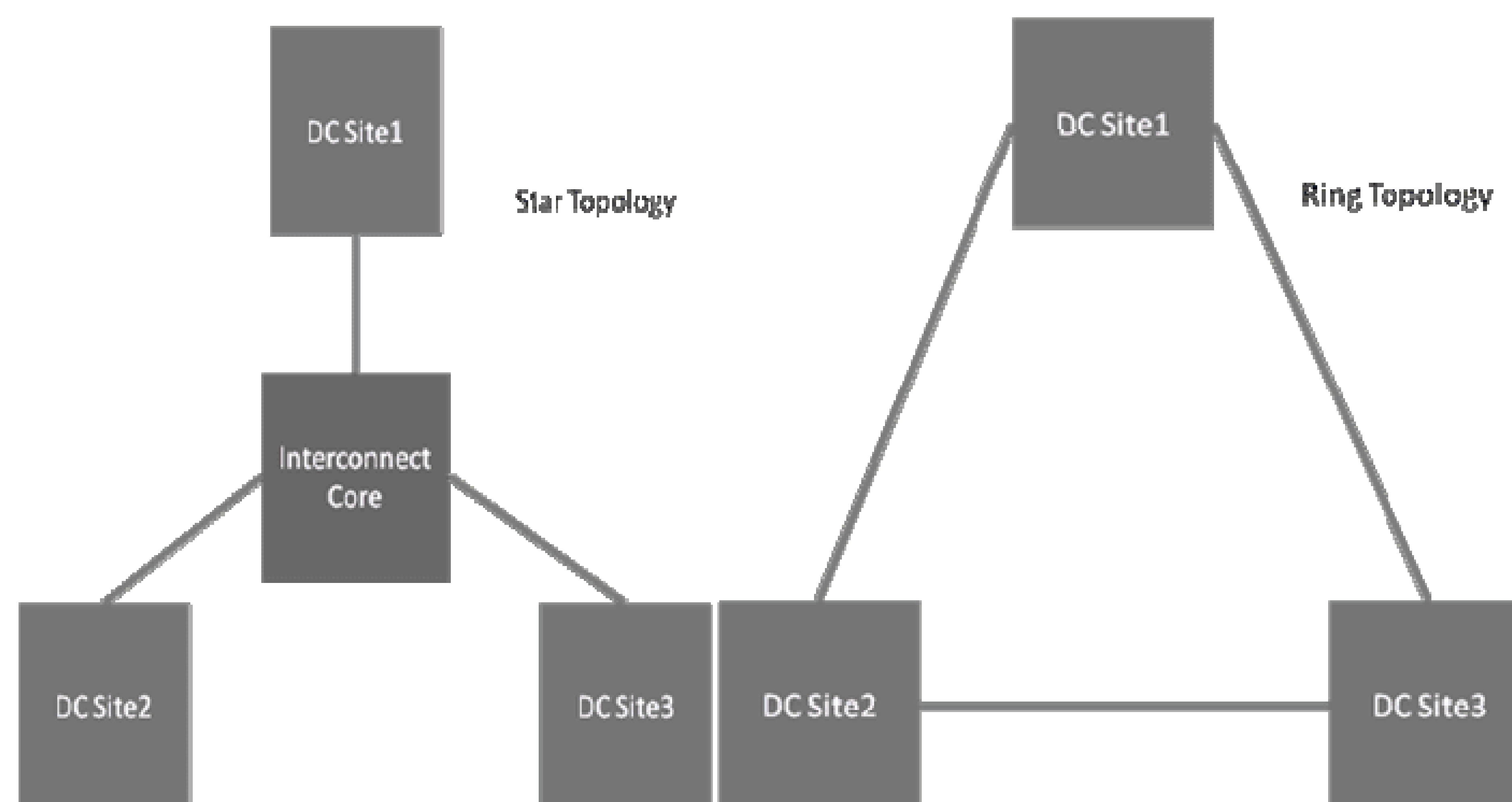
【问题 3】

为增强业务应用系统、重要数据的可用性，抵御灾难发生时带来的风险，集团需要建设两地三中心。两地三中心是指主数据中心、同城灾备及异地灾备中心。两地三中心机房为业务应用系统建设提供基础配套设施。

如果只有两个站点就不多说了，直接在两个站点的核心或汇聚设备之间拉两根光纤就 OK 了，也用不到什么特别的技术。唯一需要注意的是在两个站点之间的链路上做些报文控制，对广播和 STP 等报文限制一下发送速率和发送范围，避免一个站点的广播风暴或拓扑收敛影响到其他站点的转发。

当站点为两个以上时，理论上有两种结构可用：

星型结构：专门找几台设备作为交换核心，所有站点都通过光纤直连到此组交换核心设备上，缺点是可靠性较低，核心不工作就都连不通了，而且交换核心放置的位置也不易规划。这种结构不是值得推荐的模型。



环型结构：推荐模型，尤其在云计算这种多站点等同地位互联的大型数据中心组网下，环型结构既省设备省钱，又能提供故障保护，以后肯定会成为建设趋势。

从技术上讲星型拓扑不需要额外的二层互联技术，只部署一些报文过滤即可，可以通过链路捆绑增强站点到核心间链路故障保护和链路带宽扩展。而环型拓扑必须增加专门的协议用于防止环路风暴，同样可以部署链路捆绑以增加带宽冗余。

环型拓扑的公共标准控制协议主要是 STP 和 RPR（Resilient Packet Ring IEEE 802.17），STP 的缺点前面说了很多，RPR 更适合数据中心多站点连接的环型拓扑。另外很多厂商开发了私有协议用于环路拓扑的控制，如 EAPS（Ethernet Automatic Protection Switching，IETF RFC 3619，Extreme Networks），RRPP（Rapid Ring Protection Protocol，H3C），MRP（Metro Ring Protocol，Foundry Networks），MMRP（Multi Mater Ring Protocol，Hitachi Cable），ERP（Ethernet Ring Protection，Siemens AG）等。未来几年的云计算数据中心建设，除非在所有站点采用相同厂家的设备还有可能使用一些私有协议组环（可能性比较低），前面提到预测会以站点为单位选择不同厂家进行建设，这时就需要公共标准用于多站点互联了。在光纤直连方式下成熟技术中最好的选择就是 RPR。

根据以上分析，两地三中心的网络互联方案可考虑采用环型结构，具体拓扑结构见参考答案。

【问题 4】

存储技术经历了从基于服务器的存储（DAS），基于磁盘阵列的存储（SCSI）发展到基于网络的存储模式（NAS 及 SAN），在数据存储容量和读写速度上有较大幅度的提高，每秒传输的兆或者吉字节数和每秒完成的输入/输出量（IOPS）是存储设备的性能的两种主要参数，目前的网络存储技术大致发展为三类：DAS、NAS 以及 SAN。

（1）DAS

DAS 是一种将存储介质直接安装在服务器上或者安装在服务器外的存储方式。例如，将存储介质连接到服务器的外部 SCSI 通道上也可以认为是一种直连存储方式。

DAS 已经存在了很长时间，并且在很多情况下仍然是一种不错的存储选择。由于这种存储方式在磁盘系统和服务器之间具有很快的传输速率，在要求快速磁盘访问的情况下，DAS 仍然是一种理想的选择。更进一步地，在 DAS 环境中，运转大多数的应用程序都不会存在问题。

对于那些对成本非常敏感的企业来说，在很长一段时间内，DAS 将仍然是一种比较便宜的存储机制。当然，这是在只考虑硬件物理介质成本的情况下才有这种结论。如果与其他的技术进行一个全面的比较——考虑到管理开销和存储效率等方面的因素的话，DAS 将不再占有绝对的优势。对于那些非常小的不再需要其他存储介质的环境来说，这也是一种理想的选择。

（2）NAS

NAS 存储设备是以网络为中心面向文件服务的结构方式，NAS 存贮设备是单独作为一个文件服务器直接连接在网络上的，应用和数据存储部分不在同一服务器上，网络中设备的数据全部存贮在 NAS 存贮设备中，应用服务器通过标准 LAN 的接口与作为网络文件系统的数据服务器连接。NAS 存储系统能将数据从网络中独立出来，降低了服务器的负载，从而较好提高了整个网络的性能。

在以下两种情形中，NAS 设备是非常合适的：首要的是网页服务，其次是常用文件的存储。这两种应用都需要大量的磁盘空间，但是很少要求直接对服务器进行数据访问。相反，通过这两种类型的存储访问的大多数数据都是通过网络来实现的。

NAS 设备适合于网页服务和文件服务，而不适合于数据库存储和 Exchange 存储。这与所谓的文件级数据访问和块级数据访问有关系。在文件级访问系统中，数据的访问是通过文件名字来实现的，因为文件名字是带有一定含义的。而在块级访问系统中，数据的访问是通过数据块的地址来实现的，这个地址是特定数据存放的位置。在一个客户机/服务器的环境中，如果需要从文件服务器读取一个文件时，要指定文件，服务器完成数据块的读取工作，并且将得到的数据返回就可以了。数据库存储和 Exchange 存储在这种方式的通信过程中存在着很多问题。所以并不适合存储于 NAS 设备中。

（3）SAN

SAN 是一种以光纤通道（FiberChannel，FC）实现服务器和存储设备之间通讯的网络结构，其中的服务器和存储系统通过高带宽 FC 交换机相连，各应用工作站通过局域网访问服务器，各存储设备之间交换数据时可以不通过服务器，能有效减少大流量数据传输时发生的阻塞和冲突，较大程度减轻服务器承受的压力，具有很强的灵活性和伸缩性。作为存储解决方案中的重要一员，SAN 是最昂贵的存储选项，同时也是最复杂的选项。然而，虽然 SAN 在初始阶段需要投入大量的费用，但是 SAN 却可以提供其他解决方案所不能提供的能力，并且可以在合适的情形下可以为公司节约一定的资金。

SAN 解决方案通常会采取以下两种形式：光纤信道以及 iSCSI 或者基于 IP 的 SAN。光纤信道是 SAN 解决方案中最熟悉的类型，但是，基于 iSCSI 的 SAN 解决方案开始大量出现在市场上，与光纤通道技术相比较而言，这种技术具有良好的性能，而且价格低廉。

SAN 真正的综合了 DAS 和 NAS 两种存储解决方案的优势。例如，在一个很好的 SAN 解决方案实现中，可以得到一个完全冗余的存储网络，这个存储网络具有不同寻常的扩展性，确切地说，可以得到只有 NAS 存储解决方案才能得到的几百太字节的存储空间，但是还可以得到块级数据访问功能，而这些功能只能在 DAS 解决方案中才能得到。对于数据访问来说，还可以得到一个合理的速度，对于那些要求大量磁盘访问的操作来说，SAN 显得具有更好的性能。利用 SAN 解决方案，还可以实现存储的集中管理，从而能够充分利用那些处于空闲状态的空间。更有优势的一点是，在某些实现中，甚至可以将服务器配置为没有内部存储空间的服务器，要求所有的系统都直接从 SAN（只能

在光纤通道模式下实现）引导。这也是一种即插即用技术。

SAN 在需要容量扩容时只需要将新的 SAN 存储设备连接并入网络并进行简单的配置，即可实现在线扩容；并且 SAN 设备 RAID 组中同时损坏两块硬盘的情况下仍然可以保证数据完整不丢失，而且磁盘阵列无需重启即可更换损坏的硬盘，实现在线的数据容灾及备份性能。因此具有简易扩容及高效容错性能。

相比较 SAN 的优势和缺陷，并结合集团数据中心的建设需求，可以说采用 SAN 的存储架构对于大型国有集团是比较合理的。

参考答案

【问题 1】

（1）广域网接入区　（2）核心业务区　（3）互联网接入区　（4）办公区

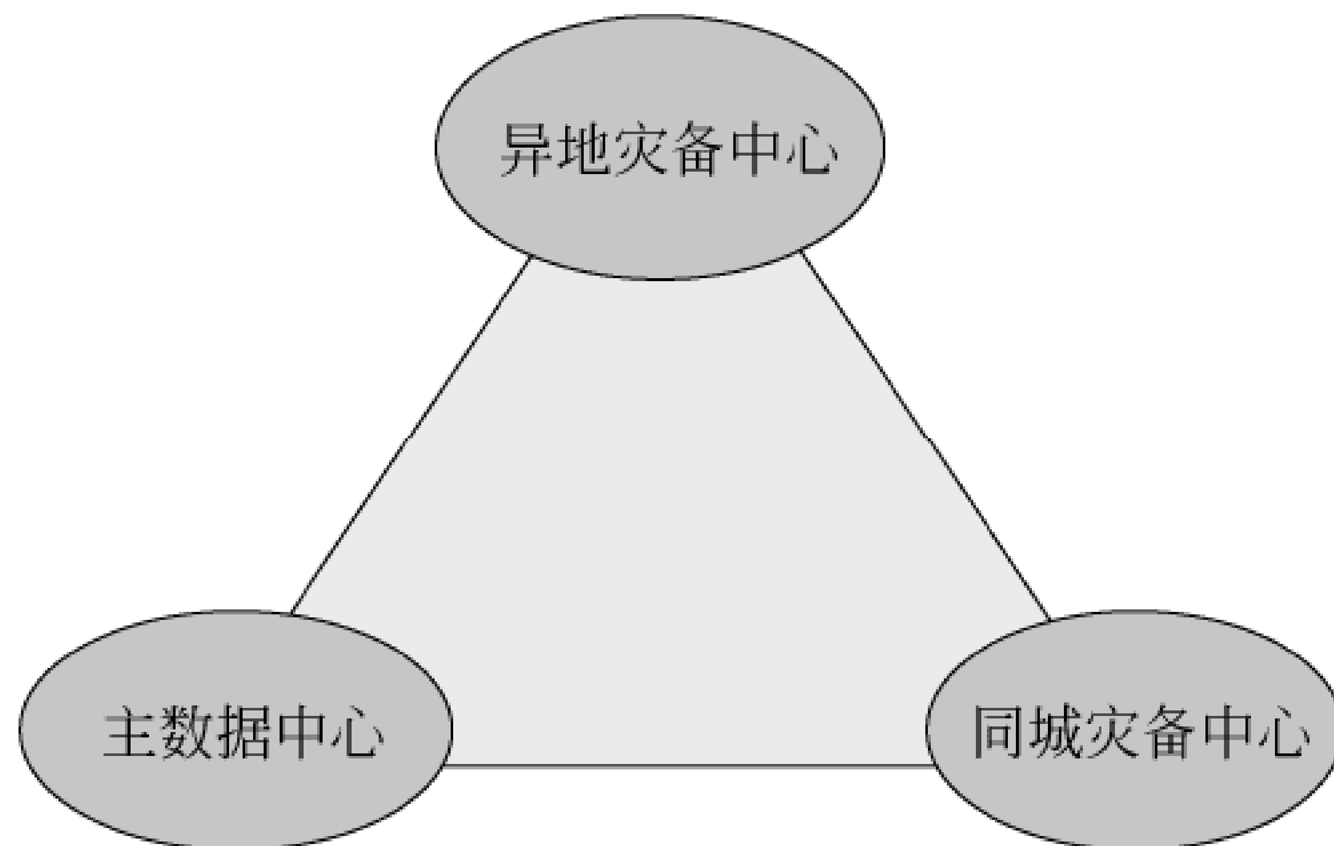
（5）运维管理区　（6）外联业务区　（7）核心交换区

【问题 2】

（1）资源池化，高效智能，面向服务，按需供给，绿色低碳。

（2）其中 IT 基础设施虚拟化技术包括网络虚拟化、服务器虚拟化及存储虚拟化。

【问题 3】



环型结构：在云计算这种多站点等同地位互联的大型数据中心组网下，环型结构不光节省设备节省费用，还能提供故障以及冗余保护。

【问题 4】

直连方式存储（Direct Attached Storage，DAS）。存储设备是通过电缆（通常是 SCSI 接口电缆）直接到服务器的。

网络附加存储（Network Attached Storage，NAS），是一种专门的数据存储技术的名称，它可以直接连接在标准的网络中（例如以太网），对异质网络用户提供了集中式数据访问服务。

存储区域网络（Storage Area Network，SAN）是一种连接外接存储设备和服务器的架构。采用包括光纤通道技术、磁盘阵列、磁带柜、光盘柜等各种技术进行实现。该架构的特点是，连接到服务器的存储设备，将被操作系统视为直接连接的存储设备。

本方案采用 SAN 的存储架构。优点是：

扩展性，不仅存储空间可以很好的得到扩充，而且还可以得到块级数据访问功能。

快速访问，对于那些要求大量磁盘访问的操作来说，SAN 具有更好的访问性能。

即插即用，可以将服务器配置为没有内部存储空间的服务器，要求所有的系统都直接从 SAN（只能在光纤通道模式下实现）引导。

相比较 SAN 的优势和缺陷，并结合集团数据中心的建设需求，可以说采用 SAN 的存储架构对于大型国有集团是比较合理的。

试题三（共 25 分）

阅读以下关于一卡通信息化建设平台的叙述，回答问题 1 至问题 4。

某部队院校早期的一卡通建设方案主要为保障校内师生的图书、食宿、医疗等服务，系统包括了一卡通专网建设、一卡通平台建设、一卡通数据中心以及校园门禁与校园网视频监控等内容。行政办公、家属区、食堂、学生宿舍、开水房等营业网点通过汇聚交换机接入到核心交换机，服务器及存储设备直接连接核心交换机，网络拓扑结构如图 3-1 所示。

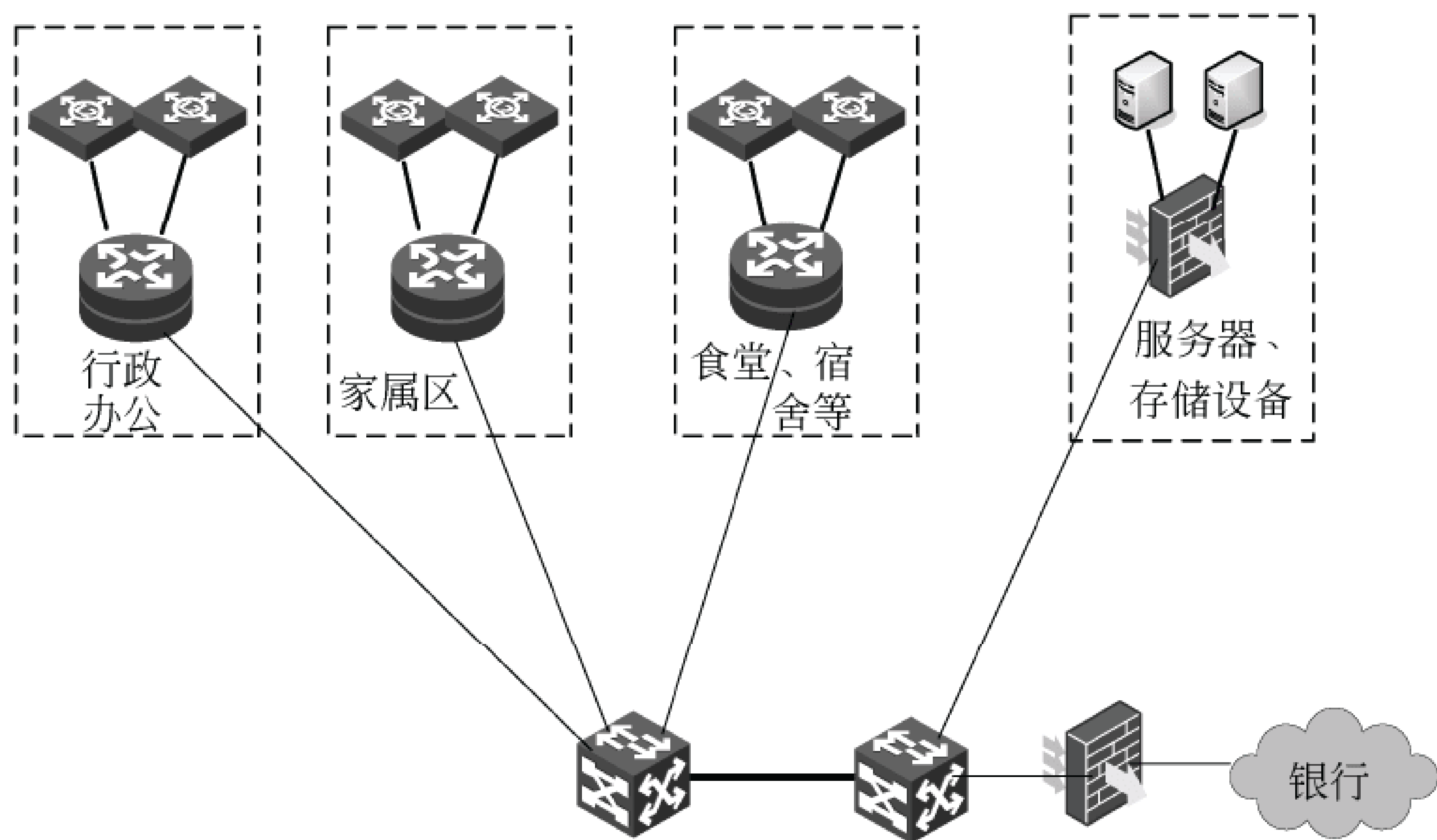


图 3-1

由于部队的医疗服务具有较高的知名度，经研究决定，扩大一卡通营业范围以方便社会人群的就医，具体安全要求如下：

（1）新增外部应用网点和分部办事处，通过安全设备来进行远程接入，要求能提供主动、实时的防护，对网络中的数据流进行逐字节的检查，对攻击性的流量进行自动拦截。

（2）由于互联网的引入，需要相应的安全措施来保障部队院校行政办公的安全。

（3）需要提供安全审计功能，来识别、存储安全相关行为。

【问题 1】（8 分）

依据一卡通业务扩大的需求及安全要求，设计解决方案，画出修改后的网络拓扑结

构，并标注采用的硬件设备及相关安全技术。

【问题 2】（6 分）

传统的防火墙存在只能对网络层和传输层进行检查，无法阻止内部人员的攻击等缺点。IDS 和 IPS 技术却能在应用层对数据流进行分析，并在网络遭受攻击之前进行报警和响应，针对部署的方式和实现的原理对 IDS 和 IPS 进行比较。

【问题 3】（6 分）

随着加密、隧道、认证等技术的发展，在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条安全的通讯线路，就可以为企业各部门提供安全的网络互联服务。针对该单位网络情况，请给出至少两种新增外部应用网点与公司核心交换机远程接入方案。

【问题 4】（5 分）

安全审计能够检测和制止对安全系统的入侵、发现计算机的滥用情况、为系统管理员提供系统运行的日志，从而能发现系统入侵行为和潜在的漏洞和对已经发生的系统攻击行为提供有效的追纠证据。请叙述安全审计的工作流程。

试题三分析

本题考查网络安全解决方案及相关知识。

【问题 1】

由于新增外部应用网点和分部办事处，通过安全设备来进行远程接入，要求能提供主动、实时的防护，对网络中的数据流进行逐字节的检查，对攻击性的流量进行自动拦截，因此需要采用具有 IPS 功能的防火墙。

由于引入了互联网，部队院校行政办公的安全需要采用网闸来与 Internet 进行物理隔离。

安全审计功能需对所有进出系统的流量进行记录，来识别、存储安全相关行为。

相应修改的拓扑结构见参考答案。

【问题 2】

IPS 的工作原理是分类、过滤和更新。和 IDS 相比，IPS 主要是对检测到的恶意代码进行核对策略，在未转发到服务器之前，将信息包或数据流拦截。由此也带来了更大的网络负载。

【问题 3】

在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条安全的通讯线路，主要的实现技术是采用 VPN 技术和端到端加密。

【问题 4】

安全审计主要的工作流程是搜集记录、分析检查、安全评估。具体流程如下：

（1）记录和搜集有关的审计信息，产生审计数据记录。

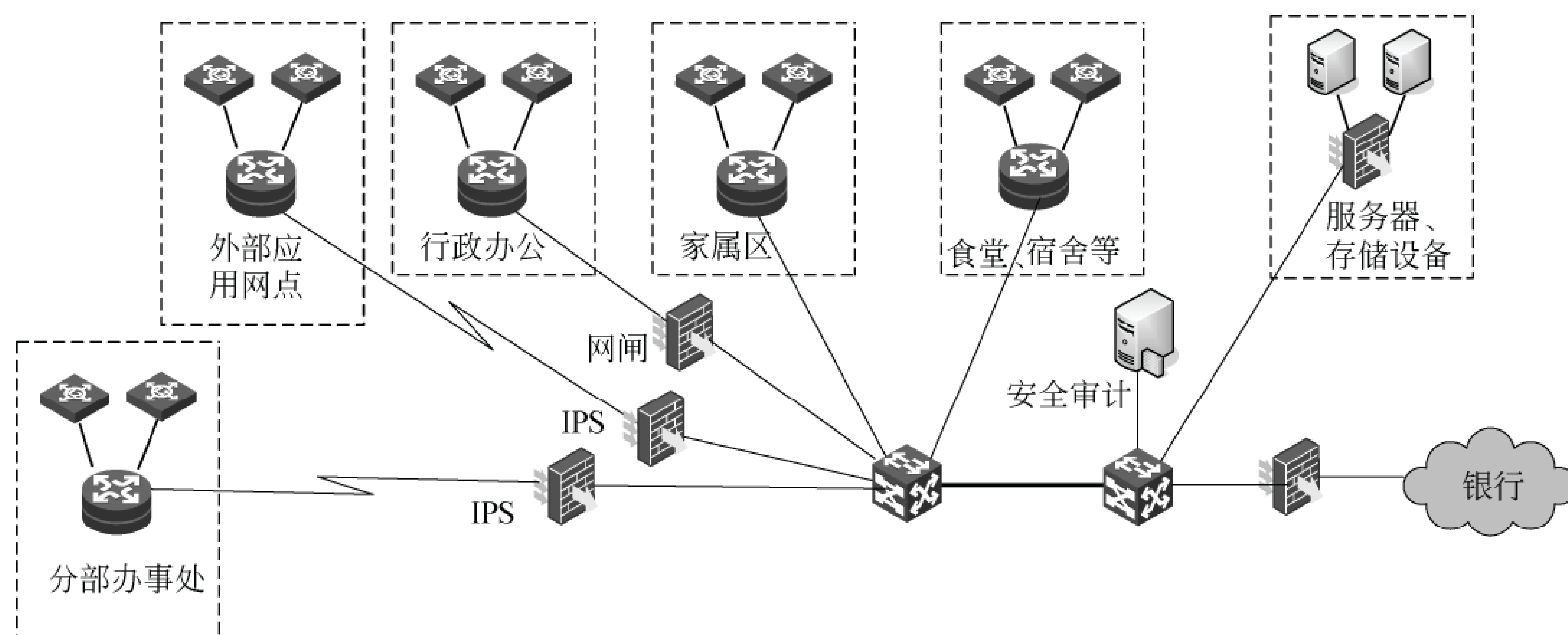
（2）对数据记录进行安全违反分析，以检查安全违反与安全入侵原因。

（3）对其分析产生相应的分析报表。

（4）评估系统安全，并提出改进意见。

参考答案

【问题 1】



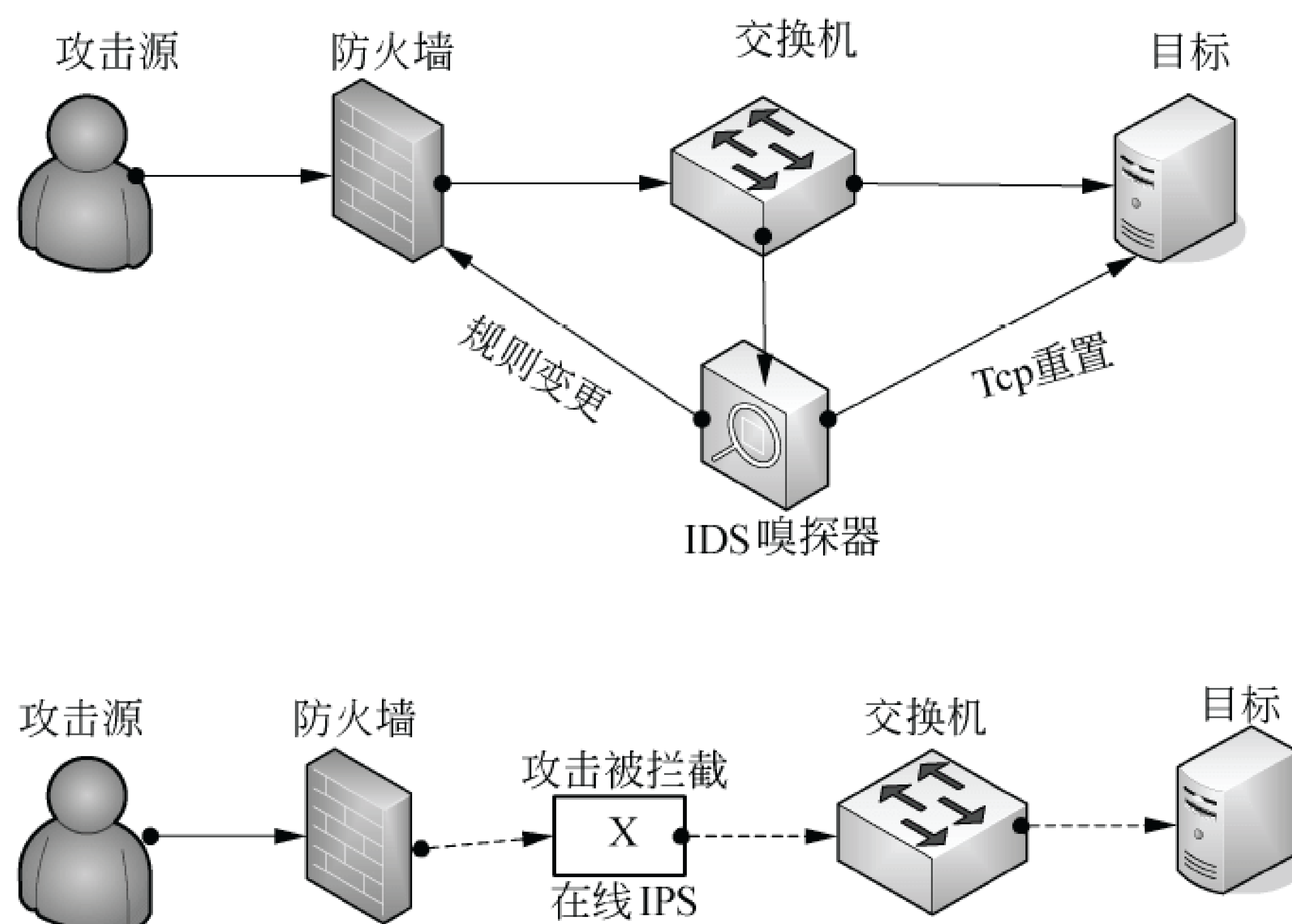
（1）外部网点要求外部网点和分部办事处能提供主动、实时的防护，对网络中的数据流进行逐字节的检查，对攻击性的流量进行自动拦截，合适的技术为 IDS 防火墙。

（2）行政办公部门要保障安全，需采用网闸进行连接。

（3）安全审计需接在核心交换机上，进行审计分析。

【问题 2】

IPS 和 IDS 的部署方式不同。串接式部署是 IPS 和 IDS 区别的主要特征，IDS 产品在网络中是旁路式工作，IPS 产品在网络中是串接式工作。



IPS 工作原理是：

（1）根据数据包头和流信息如源目的地址源目的端口和应用层关键的信息每个数据包都会被分类，同时协议类型和流量统计等信息都送到流处理模块分析、审计。

（2）根据数据报的分类，相关的过滤器将被调用，用于检查数据包的流状态信息。

（3）所有相关过滤器都是并行使用，如果任何数据报符合过滤规则，与之相关的流信息将更新，指示系统删除关于该数据流的信息。

和 IDS 相比， IPS 检测到数据流中的恶意代码，核对策略，在未转发到服务器之前，将信息包或数据流拦截。

IPS 增加了网络负载。

【问题 3】

（1）采用 VPN 技术，利用公共网络建立私有专用网络，数据通过安全的“加密隧道”在公共网络中传播，连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样。

（2）端到端加密技术，通过加密算法，保障传输数据的安全性。

【问题 4】

安全审计的工作流程如下：

（1）记录和搜集有关的审计信息，产生审计数据记录。

（2）对数据记录进行安全违反分析，以检查安全违反与安全入侵原因。

（3）对其分析产生相应的分析报表。

（4）评估系统安全，并提出改进意见

第 15 章　2012 下半年网络规划设计师下午试卷 II 写作要点

试题一　论网络规划与设计中的 VPN 技术

随着网络技术的发展和企业规模的壮大，企业在全球各地的分支机构不断增多，员工及各分支机构要求能随时随地安全可靠地访问企业内部资源，这就需要提供一种安全接入机制来保障通信以及敏感信息的安全。传统的租用专用线路的方法实现私有网络连通给企业带来很大的经济负担和网络维护成本。VPN（Virtual Private Network）技术成为当今企业实现异地多网络互连以及远程访问网络的经济安全的实现途径。

请围绕“网络规划与设计中的 VPN 技术”论题，依次对以下三个方面进行论述。

1．简要论述常用的 VPN 技术。

2．详细叙述你参与设计和实施的大中型网络项目中采用的 VPN 方案。

3．分析和评估你所采用的 VPN 方案的效果以及相关的改进措施。

写作要点

1．对 VPN 技术和方案的叙述要点

1）VPN 技术的概念

虚拟专用网（Virtual Private Network，VPN）就是建立在公用网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而通过 ISP 提供的公用网络来实现通信，其专用性表现在 VPN 之外的用户无法访问 VPN 内部的网络资源，VPN 内部用户之间可以实现安全通信。

2）实现 VPN 的关键技术

隧道技术、加解密技术、密钥管理技术、身份认证技术。

3）VPN 的解决方案

（1）内联网 VPN（Intranet VPN）：企业内部虚拟专用网也叫内联网 VPN，用于实现企业内部各个 LAN 之间的安全互联。

（2）外联网 VPN（Extranet VPN）：企业外部虚拟专用网也叫外联网 VPN，用于实现企业与客户、供应商和其他相关团体之间的互联互通。

（3）远程接入 VPN（Access VPN）：解决远程用户访问企业内部网络的传统方法是采用长途拨号方式接入企业的网络访问服务器（NAS）。这种访问方式的缺点是通信成本高，必须支付价格不菲的长途电话费，而且 NAS 和调制解调器的设备费用，以及租用接入线路的费用也是一笔很大的开销。采用远程接入 VPN 就可以省去这些费用。如果企业内部人员有移动或远程办公的需要，或者商家要提供 B2C 的安全访问服务，可以采用 Access VPN。

4）虚拟专用网 VPN 的协议实现

隧道协议（例如 PPTP 和 L2TP），把数据封装在点对点协议（PPP）的帧中在互联网上传输，创建隧道的过程类似于在通信双方之间建立会话的过程，需要就地址分配、加密、认证和压缩参数等进行协商，隧道建立后才进行数据传输。

IPSec（IP Security）是 IETF 定义的一组协议，用于增强 IP 网络层安全。IPSec VPN 是在网络层建立安全隧道，适用于建立固定的虚拟专用网。

安全套接层（Secure Socket Layer，SSL）是传输层安全协议，用于实现 Web 安全通信。SSL 的安全连接是通过应用层的 Web 连接建立的，更适合移动用户远程访问公司的虚拟专用网。

2．叙述自己参与设计和实施的计算机网络项目，该项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量，说明项目中选用的 VPN 方案以及选用该方案的理由。

3．对选择的网络系统设计中 VPN 方案的效果以及需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

试题二　校园网设计关键技术及解决方案

校园网的建设有利于校内的资源共享与信息交换，有利于学校与外界的资源共享和信息共享。校园网的规划、设计、硬件建设、软件建设以及已有网络设备的使用及调优，都要从全局、长远的角度出发，充分考虑网络的安全性、易用性、可靠性和经济性等。资源调优、光纤连接和无线解决方案是保障校园网络可靠易用的几项关键技术。

请围绕“校园网设计关键技术及解决方案”论题，依次对以下三个方面进行论述。

1．以你负责规划、设计及实施的校园网项目为例，概要叙述针对实际需求的设计要点，以及如何充分利用已有的软硬件，或对现有硬件资源的调优措施。

2．具体讨论在校园网/企业网网络规划与设计中高性能的光纤连接关键技术、采用的无线技术及解决方案。

3．具体讨论在上述关键技术的实施过程中遇到的问题和解决措施，以及实际运行效果。

写作要点

1．以你负责规划、设计及实施的校园网项目为例，概要叙述针对实际需求的设计要点，以及如何充分利用已有的软硬件，或对现有硬件资源的调优措施。

（1）叙述自己参与设计和实施的计算机网络项目。该项目应有一定的规模，自己的主要工作应有一定的分量。

（2）项目中对软硬件的重新利用及调优方案。已有软硬件资源不适合整个网络环境的应该淘汰，可以用在要求较低环境中的可重利用，更高要求的要重新购置。

2．具体讨论在校园网/企业网网络规划与设计中光纤连接关键技术、采用的无线技术及解决方案。

在光纤连接技术方面：

（1）光纤连接的总体环境。在光纤网络部署时首先要考虑距离、所要求达到的速率。

（2）介质选择。依据距离、速率以及成本选择采用单模还是多模，考虑室内或是室外选择不同的光纤。

（3）接口模块与成本预算。在介质选择完成后，需要考虑光纤接口模块，计算成本。

（4）冗余。考虑到光纤日后扩展及链路备份，需要冗余链路。

在无线技术方面：

（1）无线网络需求。不同的无线网络环境需要不同的速率和安全要求，需要描述所涉及网络的要求环境。

（2）采用的无线局域网络标准。不同的速率和安全要求需要采用不同的标准，注意选择标准与需求相匹配。

（3）无线网络的网络结构及覆盖范围。

（4）选用的无线接入设备，包括无线路由器、AP 等。

3．具体讨论在上述关键技术的实施过程中遇到的问题和解决措施，以及实际运行效果。

（1）在光纤连接和无线技术使用过程中遇到的问题及解决措施。

（2）网络部署完成后实际的效果、达到的性能。

第 16 章　2013 下半年网络规划设计师上午试题分析与解答

试题（1）

活动定义是项目时间管理中的过程之一，__（1）__是进行活动定义时通常使用的一种工具。

（1）A．Gantt 图　　B．活动图

C．工作分解结构（WBS）　　D．PERT 图

试题（1）分析

项目时间管理包括使项目按时完成所必须的管理过程。项目时间管理中的过程包括：活动定义、活动排序、活动的资源估算、活动历时估算、制定进度计划以及进度控制。为了得到工作分解结构（Work Breakdown Structure，WBS）中最底层的交付物，必须执行一系列的活动，对这些活动的识别以及归档的过程就叫做活动定义。

参考答案

（1）C

试题（2）、（3）

基于 RUP 的软件过程是一个迭代过程。一个开发周期包括初始、细化、构建和移交四个阶段，每次通过这四个阶段就会产生一代软件，其中建立完善的架构是__（2）__阶段的任务。采用迭代式开发，__（3）__。

（2）A．初始　　B．细化　　C．构建　　D．移交

（3）A．在每一轮迭代中都要进行测试与集成

B．每一轮迭代的重点是对特定的用例进行部分实现

C．在后续迭代中强调用户的主动参与

D．通常以功能分解为基础

试题（2）、（3）分析

RUP 中的软件过程在时间上被分解为 4 个顺序的阶段，分别是初始阶段、细化阶段、构建阶段和移交阶段。

初始阶段的任务是为系统建立业务模型并确定项目的边界。细化阶段的任务是分析问题领域，建立完善的架构，淘汰项目中最高风险的元素。在构建阶段，要开发所有剩余的构件和应用程序功能，把这些构件集成为产品。移交阶段的重点是确保软件对最终用户是可用的。

基于 RUP 的软件过程是一个迭代过程，通过初始、细化、构建和移交 4 个阶段就是一个开发周期，每次经过这 4 个阶段就会产生一代产品，在每一轮迭代中都要进行测试

与集成。

参考答案

（2）B　（3）A

试题（4）

以下关于白盒测试方法的叙述，不正确的是（4）。

（4）A. 语句覆盖要求设计足够多的测试用例，使程序中每条语句至少被执行一次
B. 与判定覆盖相比，条件覆盖增加对符合判定情况的测试，增加了测试路径
C. 判定/条件覆盖准则的缺点是未考虑条件的组合情况
D. 组合覆盖要求设计足够多的测试用例，使得每个判定中条件结果的所有可能组合最多出现一次

试题（4）分析

白盒测试也称为结构测试，主要用于软件单元测试阶段，测试人员按照程序内部逻辑结构设计测试用例，检测程序中的主要执行通路是否都能按预定要求正确工作。白盒测试方法主要有控制流测试、数据流测试和程序变异测试等。

控制流测试根据程序的内部逻辑结构设计测试用例，常用的技术是逻辑覆盖。主要的覆盖标准有语句覆盖、判定覆盖、条件覆盖、条件/判定覆盖、条件组合覆盖、修正的条件/判定覆盖和路径覆盖等。

语句覆盖是指选择足够多的测试用例，使得运行这些测试用例时，被测程序的每个语句至少执行一次。

判定覆盖也称为分支覆盖，它是指不仅每个语句至少执行一次，而且每个判定的每种可能的结果（分支）都至少执行一次。

条件覆盖是指不仅每个语句至少执行一次，而且使判定表达式中的每个条件都取得各种可能的结果。

条件/判定覆盖同时满足判定覆盖和条件覆盖。它的含义是选取足够的测试用例，使得判定表达式中每个条件的所有可能结果至少出现一次，而且每个判定本身的所有可能结果也至少出现一次。

条件组合覆盖是指选取足够的测试用例，使得每个判定表达式中条件结果的所有可能组合至少出现一次。

修正的条件/判定覆盖。需要足够的测试用例来确定各个条件能够影响到包含的判定结果。

路径覆盖是指选取足够的测试用例，使得程序的每条可能执行到的路径都至少经过一次（如果程序中有环路，则要求每条环路路径至少经过一次）。

参考答案

（4）D

试题（5）

某企业拟生产甲、乙、丙、丁四个产品。每个产品必须依次由设计部门、制造部门和检验部门进行设计、制造和检验，每个部门生产产品的顺序是相同的。各产品各工序所需的时间如下表：

项目	设计（天）	制造（天）	检验（天）
甲	13	15	20
乙	10	20	18
丙	20	16	10
丁	8	10	15

只要适当安排好项目实施顺序，企业最快可以在<u>（5）</u>天全部完成这四个项目。

（5）A．84　　B．86　　C．91　　D．93

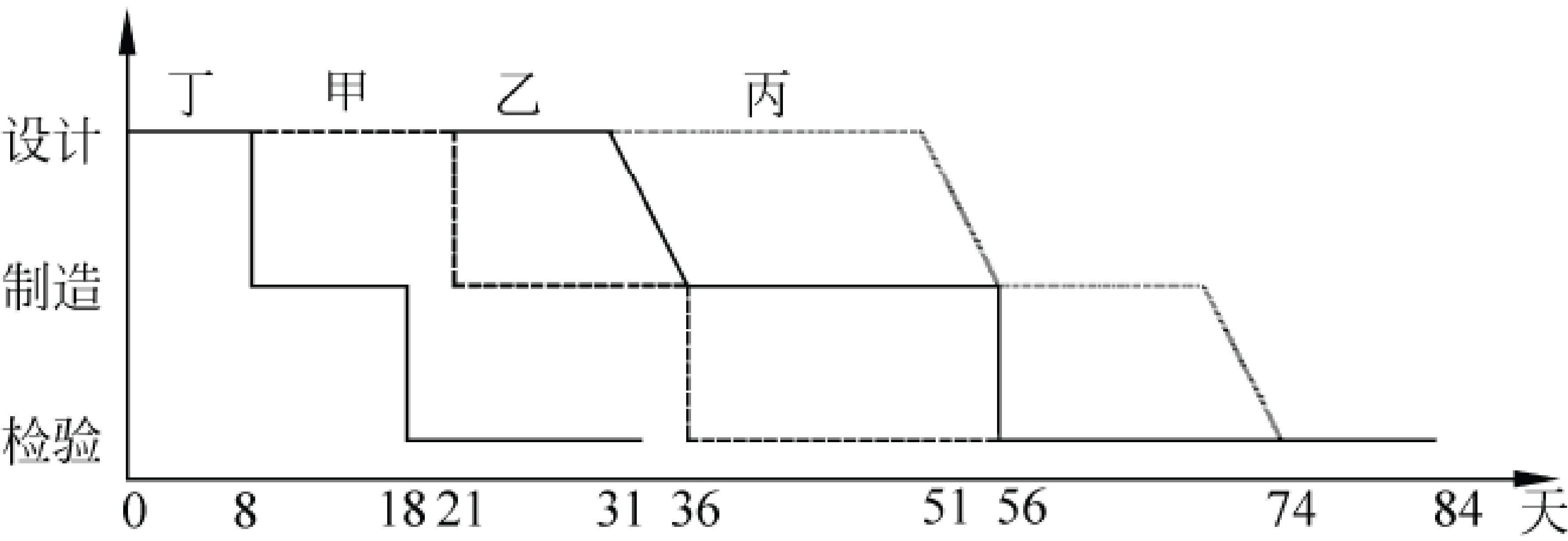
试题（5）分析

本题考查数学应用的能力（优化运筹）。

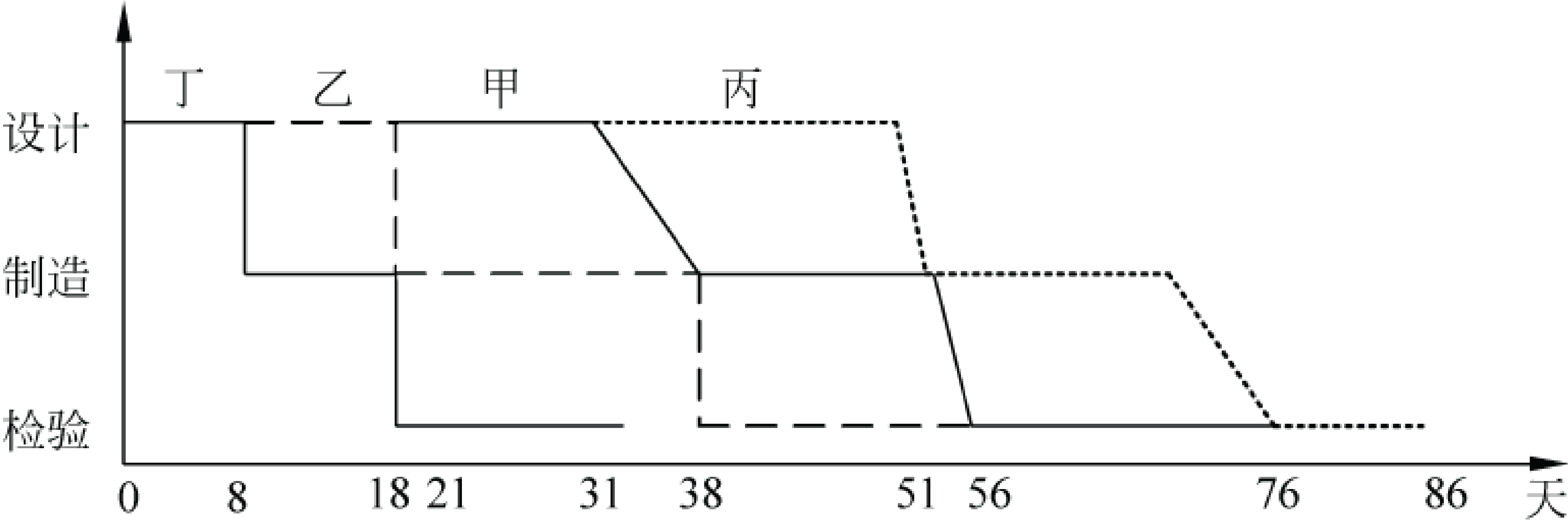
节省时间的安排方法必然是紧随衔接和尽可能并行安排生产。

第 1 个产品的设计和最后 1 个产品的检验是无法与其他工作并行进行的，因此，应安排“首个设计时间+末个检验时间”尽可能短。为此，应先安排生产丁，最后安排生产丙。

如果按丁、甲、乙、丙顺序实施，则共需 84 天，如下图所示。



如果按丁、乙、甲、丙顺序实施，则共需 86 天，如下图所示。



参考答案

（5）A

试题（6）

下列关于面向对象软件测试的说法中，正确的是__（6）__。

（6）A. 在测试一个类时，只要对该类的每个成员方法都进行充分的测试就完成了对该类充分的测试

B. 存在多态的情况下，为了达到较高的测试充分性，应对所有可能的绑定都进行测试

C. 假设类 B 是类 A 的子类，如果类 A 已经进行了充分的测试，那么在测试类 B 时不必测试任何类 B 继承自类 A 的成员方法

D. 对于一棵继承树上的多个类，只有处于叶子节点的类需要测试

试题（6）分析

面向对象系统的测试目标与传统信息系统的测试目标是一致的，但面向对象系统的测试策略与传统结构化系统的测试策略有很大的不同，这主要体现在两个方面，分别是测试的焦点从模块移向了类，以及测试的视角扩大到了分析和设计模型。

与传统的结构化系统相比，面向对象系统具有三个明显特征，即封装性、继承性与多态性。封装性决定了面向对象系统的测试必须考虑到信息隐蔽原则对测试的影响，以及对象状态与类的测试序列，因此在测试一个类时，仅对该类的每个方法进行测试是不够的；继承性决定了面向对象系统的测试必须考虑到继承对测试充分性的影响，以及误用引起的错误；多态性决定了面向对象系统的测试必须考虑到动态绑定对测试充分性的影响、抽象类的测试以及误用对测试的影响。

参考答案

（6）B

试题（7）

以下关于自顶向下开发方法的叙述中，正确的是__（7）__。

（7）A. 自顶向下过程因为单元测试而比较耗费时间

B. 自顶向下过程可以更快地发现系统性能方面的问题

C. 相对于自底向上方法，自顶向下方法可以更快地得到系统的演示原型

D. 在自顶向下的设计中，如发现了一个错误，通常是因为底层模块没有满足其规格说明（因为高层模块已经被测试过了）

试题（7）分析

自顶向下方法是一种决策的策略。软件开发涉及作什么决策、如何决策和决策顺序等决策问题。

自顶向下方法在任何时刻所作的决定都是当时对整个设计影响最大的那些决定。如果把所有决定分组或者分级，那么决策顺序是首先作最高级的决定，然后依次地作较低

级的决定。同级的决定则按照随机的顺序或者按别的方法。一个决定的级别是看它距离要达到的最终目的（因此是软件的实际实现）的远近程度。从问题本身来看，或是由外（用户所见的）向内（系统的实现）看，以距离实现近的决定为低级决定，远的为高级决定。

在这个自顶向下的过程中，一个复杂的问题（任务）被分解成若干个较小较简单的问题（子任务），并且一直继续下去，直到每个小问题（子任务）都简单到能够直接解决（实现）为止。

自顶向下方法的优点是：

- 可为企业或机构的重要决策和任务实现提供信息。
- 支持企业信息系统的整体性规划，并对系统的各子系统的协调和通信提供保证。
- 方法的实践有利于提高企业人员的整体观察问题的能力，从而有利于寻找到改进企业组织的途径。

自顶向下方法的缺点是：

- 对系统分析和设计人员的要求较高。
- 开发周期长，系统复杂，一般属于一种高成本、大投资的工程。
- 对于大系统而言，自上而下的规划对于下层系统的实施往往缺乏约束力。
- 从经济角度来看，很难说自顶向下的做法在经济上市合算的。

参考答案

（7）C

试题（8）、（9）

企业信息集成按照组织范围分为企业内部的信息集成和外部的信息集成。在企业内部的信息集成中，<u>（8）</u>实现了不同系统之间的互操作，使得不同系统之间能够实现数据和方法的共享；<u>（9）</u>实现了不同应用系统之间的连接、协调运作和信息共享。

（8）A．技术平台集成　　B．数据集成
　　C．应用系统集成　　D．业务过程集成

（9）A．技术平台集成　　B．数据集成
　　C．应用系统集成　　D．业务过程集成

试题（8）、（9）分析

本题考查企业信息集成的基础知识。

企业信息集成是指企业在不同应用系统之间实现数据共享，即实现数据在不同数据格式和存储方式之间的转换、来源不同、形态不一、内容不等的信息资源进行系统分析、辨清正误、消除冗余、合并同类，进而产生具有统一数据形式的有价值信息的过程。企业信息集成是一个十分复杂的问题，按照组织范围来分，分为企业内部的信息集成和外部的信息集成两个方面。按集成内容，企业内部的信息集成一般可分为以下四个方面：技术平台集成，数据集成，应用系统集成和业务过程集成。其中，应用系统集成是实现

不同系统之间的互操作，使得不同应用系统之间能够实现数据和方法的共享；业务过程集成使得在不同应用系统中的流程能够无缝连接，实现流程的协调运作和流程信息的充分共享。

参考答案

（8）C　（9）D

试题（10）

以下关于为撰写学术论文引用他人资料的说法，__（10）__是不正确的。

（10）A．既可引用发表的作品，也可引用未发表的作品

B．只能限于介绍、评论或为了说明某个问题引用作品

C．只要不构成自己作品的主要部分，可引用资料的部分或全部

D．不必征得著作权人的同意，不向原作者支付合理的报酬

试题（10）分析

作品实际上是在吸纳和借鉴前人的多种智力成果的基础上而逐渐创作出来的。为了让作品能被更多的人所传播、利用与掌握，以有利于技术和文化的进步、发展，著作权法一方面向著作人授予精神、经济专有权利并保护这些权利所带来的利益，同时又对权利人行使其专有权利给予了一定的限制，便于公众接触、使用作品，为进一步提高技术和文化提供条件。

著作权的限制主要体现在合理使用、法定许可使用两个方面。合理使用是指在特定的条件下，法律允许他人自由使用享有著作权的作品而不必征得著作权人的同意，也不必向著作权人支付报酬的行为，但应当指明作者姓名、作品名称，并且不得侵犯著作权人依照本法享有的其他权利。法定许可使用是指除著作权人声明不得使用外，使用人在未经著作权人许可的情况下，在向著作权人支付报酬时，指明著作权人姓名、作品名称，并且不侵犯著作权人依法享有的合法权利的情况下进行使用的行为。法定许可使用与合理使用的相同处在于：以促进社会公共利益、限制著作权人权利为目的；使用的作品限于已发表作品；无须征得著作权人的同意，但必须注明作者姓名、作品名称。我国著作权法第二十二条具体规定了合理使用的 12 种情形，一种情形是“为介绍、评论某一作品或者说明某一问题，在作品中适当引用他人已经发表的作品。”题干所述“引用”是合理使用的一种，引用目的仅限于介绍、评论某一作品或者说明某一问题，所引用部分不能构成引用人作品的主要部分或者实质部分。

参考答案

（10）A

试题（11）

在 ISO/OSI 参考模型中，传输层采用三次握手协议建立连接，采用这种协议的原因是__（11）__。

（11）A．为了在网络服务不可靠的情况下也可以建立连接

B．防止因为网络失效或分组重复而建立错误的连接
C．它比两次握手协议更能提高连接的可靠性
D．为了防止黑客进行 DoS 攻击

试题（11）分析

传输层协议使用三次握手过程建立连接，这种方法可以防止出现错误连接。大部分错误连接是由于迟到的或网络中存储的连接请求引起的。由于三次握手过程强调连接的双方都要提出自己的连接请求标识，也要应答对方的连接请求标识，所以不会受到过期的连接请求的干扰。

参考答案

（11）B

试题（12）

设卫星信道的传播延迟为 270ms，数据速率为 64kb/s，帧长 4000 比特，采用停等 ARQ 协议，则信道的最大利用率为__（12）__。

（12）A．0.480　　B．0.125　　C．0.104　　D．0.010

试题（12）分析

停等 ARQ 协议的信道利用率为

$$E=\frac{1}{2a+1}$$

其中 a= t_p / t_f，t_p 为信道延迟，t_f 为帧发送或接收时间，这是在停等协议下链路的最高利用率，也可以认为是停等协议的效率。

本题中，卫星信道的传播延迟 t_p=270ms，t_f=4000÷64=62.5ms，所以：

$$a=270 / 62.5=4.32$$

于是

$$E=\frac{1}{2a+1}=\frac{1}{2\times4.32+1}=\frac{1}{9.64}=0.104$$

参考答案

（12）C

试题（13）、（14）

在相隔 2000km 的两地间通过电缆以 4800b/s 的速率传送 3000 比特长的数据包，从开始发送到接收完数据需要的时间是__（13）__，如果用 50kb/s 的卫星信道传送，则需要的时间是__（14）__。

（13）A．480ms　　B．645ms　　C．630ms　　D．635ms
（14）A．70ms　　B．330ms　　C．500ms　　D．600ms

试题（13）、（14）分析

从开始发送到接收完数据需要的时间为信道传播延迟+数据包的接收（或发送）时间。通过电缆传送数据包的传播延迟=2000km÷200m/μs=10ms，数据包的接收时间=

3000÷4800=625ms，所以从开始发送到接收完数据需要的时间为 635ms。

通过卫星信道传送数据包时，信道传播延迟=270ms，数据包的接收时间=3000÷50k=60ms，所以从开始发送到接收完数据需要的时间为 330ms。

参考答案

（13）D （14）B

试题（15）

10 个 9.6kb/s 的信道按时分多路复用在一条线路上传输，在统计 TDM 情况下，假定每个子信道只有 30%的时间忙，复用线路的控制开销为 10%，那么复用线路的带宽应该是 （15） 。

（15）A. 32kb/s B. 64kb/s C. 72kb/s D. 96kb/s

试题（15）分析

根据题意计算如下：9.6kb/s×10×30%÷90%=32kb/s

参考答案

（15）A

试题（16）

关于 HDLC 协议的流量控制机制，下面的描述中正确的是 （16） 。

（16）A. 信息帧（I）和管理帧（S）的控制字段都包含发送顺序号

B. 当控制字段 C 为 8 位长时，发送顺序号的变化范围是 0～127

C. 发送完一个信息帧（I）后，发送器就将其发送窗口向前移动一格

D. 接收器成功接收到一个帧后，就将其接收窗口后沿向前移动一格

试题（16）分析

HDLC 协议采用固定大小的滑动窗口协议进行流量控制。信息帧和控制帧是编号帧，管理帧是无编号帧；当控制字段为 8 位长时，帧编号只有 3 位长，取值范围为 0～7；发送器只有在收到肯定应答后才能向前移动窗口；接收器成功收到一个帧后，就将其窗口向前移动一格，并送回肯定应答信号。

参考答案

（16）D

试题（17）、（18）

由域名查询 IP 地址的过程分为递归查询和迭代查询两种，其中递归查询返回的结果为 （17） ，而迭代查询返回的结果是 （18） 。

（17）A. 其他服务器的名字或地址

B. 上级域名服务器的地址

C. 域名所对应的 IP 地址或错误信息

D. 中介域名服务器的地址

（18）A. 其他服务器的名字或地址

B．上级域名服务器的地址

C．域名所对应的 IP 地址或错误信息

D．中介域名服务器的地址

试题（17）、（18）分析

IP 地址的解析过程分为递归查询和迭代查询两种，递归查询返回的结果为域名对应的 IP 地址或错误信息，而迭代查询返回的结果是其他服务器（包括中介域名服务器和上级域名服务器）的名字或地址。

参考答案

（17）C　（18）A

试题（19）

为了满足不同用户的需求，可以把所有自动获取 IP 地址的主机划分为不同的类别，下面的选项列出的划分类别的原则中合理的是__（19）__。

（19）A．移动用户划分到租约期较长的类

B．固定用户划分到租约期较短的类

C．远程访问用户划分到默认路由类

D．服务器划分到租约期最短的类

试题（19）分析

在配置动态 IP 地址时对用户进行分类的原则是：移动用户划分到租约期较短的类别；固定用户划分到租约期较长的类别；远程访问用户划分到默认路由类；服务器分配静态 IP 地址。

参考答案

（19）C

试题（20）

TCP 协议在建立连接的过程中可能处于不同的状态，用 netstat 命令显示出 TCP 连接的状态为 SYN_SEND，则这个连接正处于__（20）__。

（20）A．监听对方的建立连接请求　　B．已主动发出连接建立请求

C．等待对方的连接释放请求　　D．收到对方的连接建立请求

试题（20）分析

TCP 的连接状态如图 1 所示，由图看出，当 TCP 实体主动发出连接请求（SYN）后处于 SYN_SEND 状态。

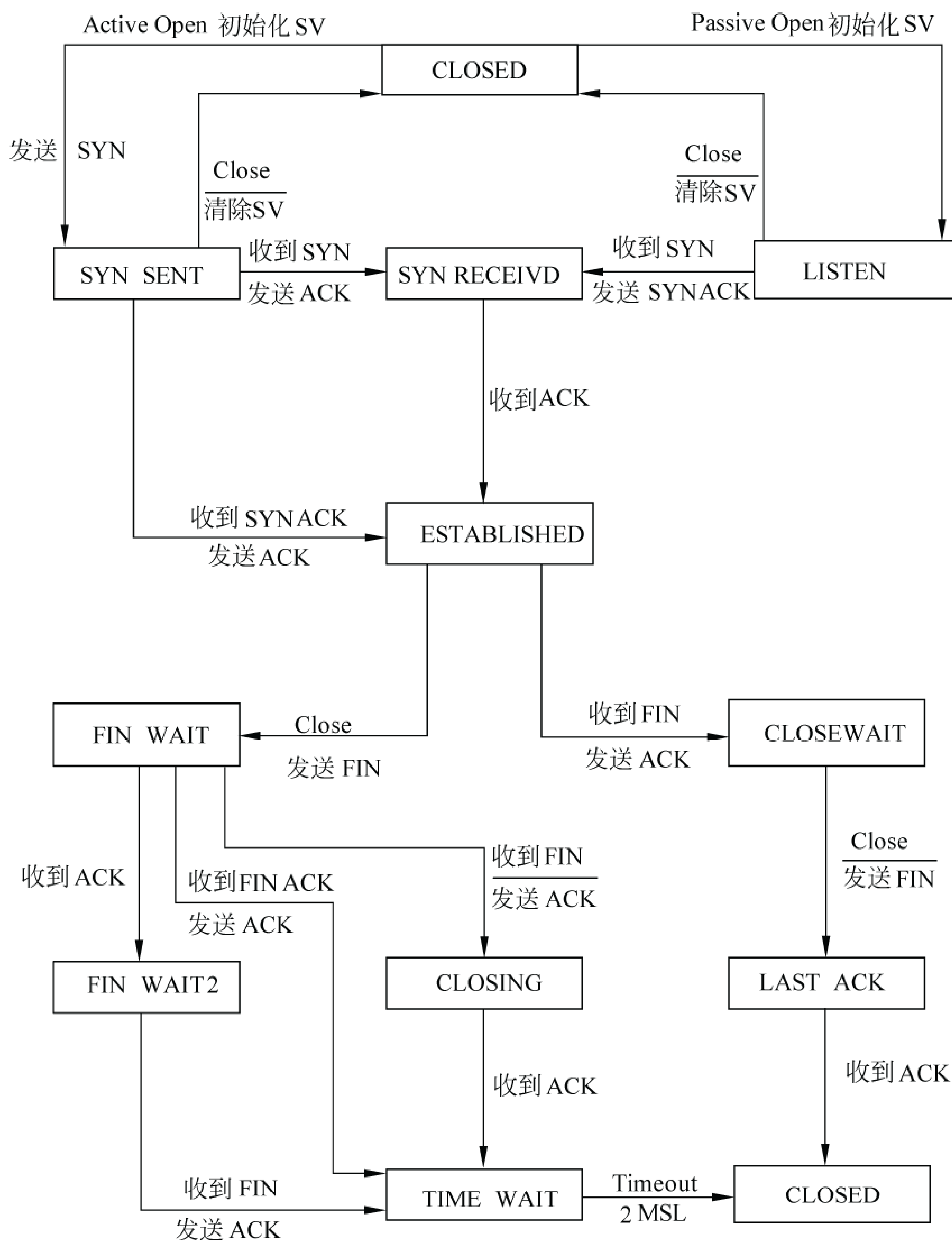
参考答案

（20）B

试题（21）

自动专用 IP 地址（Automatic Private IP Address，APIPA）是 IANA 保留的一个地址

块，其地址范围是＿（21）＿。



（21）A．A 类地址块 10.254.0.0～10.254.255.255

B．A 类地址块 100.254.0.0～100.254.255.255

C．B 类地址块 168.254.0.0～168.254.255.255

D．B 类地址块 169.254.0.0～169.254.255.255

试题（21）分析

自动专用 IP 地址 APIPA 的范围是 B 类地址块 169.254.0.0～169.254.255.255。

参考答案

（21）D

试题（22）

下面关于 GPRS 接入技术的描述中，正确的是（22）。

（22）A．GPRS 是一种分组数据业务

B．GPRS 是一种第三代移动通信标准

C．GPRS 提供的数据速率可以达到 1Mb/s

D．GPRS 是一种建立在 CDMA 网络上的数据传输技术

试题（22）分析

通用分组无线业务 GPRS（General Packet Radio Service）是一种 2.5G 移动通信系统。2.5G 系统能够提供 3G 系统中才有的一些功能，例如分组交换业务，也能共享 2G 时代开发出来的 TDMA 或 CDMA 网络。GPRS 分组网络重叠在 GSM 网络之上，利用GSM 网络中未使用的TDMA信道，为用户提供中等速度的移动数据业务。

GPRS 是基于分组交换的技术，多个用户可以共享带宽，每个用户只有在传输数据时才会占用信道，所有的可用带宽可以立即分配给当前发送数据的用户，适合于 Web 浏览、E-mail 收发和即时消息那样的共享带宽的间歇性数据传输业务。通常，GPRS 系统是按交换的字节数计费，而不是连接时间计费。GPRS 系统支持IP协议和PPP协议。理论上的分组交换速度大约是 170kb/s，而实际速度只有 30～70kb/s。

对 GPRS 的射频部分进行改进的技术方案称为增强数据速率的 GSM 演进（Enhanced Data rates for GSM Evolution，EDGE）。EDGE又称为增强型 GPRS（EGPRS），可以工作在已经部署 GPRS 的网络上，只需要对手机和基站设备做一些简单的升级。EDGE被认为是 2.75G 技术，采用8PSK的调制方式代替了 GSM 使用的高斯最小移位键控（GMSK）调制方式，使得一个码元可以表示 3 比特信息。理论上说，EDGE 提供的数据速率是 GSM 系统的 3 倍。2003 年 EDGE 被引入北美的 GSM 网络，支持从 20～200kb/s 的高速数据传输，最大数据速率取决于同时分配到的 TDMA 帧的时隙的多少。

参考答案

（22）A

试题（23）

IEEE 802.3 规定的 CSMA/CD 协议可以利用多种监听算法来减小发送冲突的概率，下面关于各种监听算法的描述中，正确的是（23）。

（23）A．非坚持型监听算法有利于减少网络空闲时间

B．坚持型监听算法有利于减少冲突的概率

C．P 坚持型监听算法无法减少网络的空闲时间

D．坚持型监听算法能够及时抢占信道

试题（23）分析

以太网的监听算法分为 3 种：

非坚持型监听算法可以最大限度地减少冲突概率，但是可能会延迟发送，引起带宽的浪费；坚持型监听算法能及时抢占信道，但是会增加冲突的概率。P-坚持型监听算法既可以及时抢占信道，也不会增加冲突的概率，但是算法复杂，需要根据网络的负载情况进行仔细的调整。

参考答案

（23）D

试题（24）

采用以太网链路聚合技术将__（24）__。

（24）A. 多个逻辑链路组成一个物理链路
B. 多个逻辑链路组成一个逻辑链路
C. 多个物理链路组成一个物理链路
D. 多个物理链路组成一个逻辑链路

试题（24）分析

IEEE 802.3ad 定义了链路聚合控制协议（Link Aggregation Control Protocol，LACP），它的功能是将多个物理链路聚合成一个逻辑链路。链路汇聚技术可以将多个链路绑定在一起，形成一条高速链路，以达到更高的带宽，并实现链路备份和负载均衡。

参考答案

（24）D

试题（25）、（26）

RIP 是一种基于__（25）__的内部网关协议，在一条 RIP 通路上最多可包含的路由器数量是__（26）__。

（25）A. 链路状态算法 B. 距离矢量算法
C. 集中式路由算法 D. 固定路由算法

（26）A. 1 个 B. 16 个 C. 25 个 D. 无数个

试题（25）、（26）分析

RIP 是一种基于距离矢量算法的内部网关协议，在一条 RIP 通路上最多可包含的路由器数量是 16 个。

参考答案

（25）B （26）B

试题（27）

关于实现 QoS 控制的资源预约协议 RSVP，下面的描述中正确的是__（27）__。

（27）A. 由发送方向数据传送路径上的各个路由器预约带宽资源
B. 由发送方向接收方预约数据缓冲资源

C. 由接收方和发送方共同商定各条链路上的资源分配

D. 在数据传送期间，预约的路由信息必须定期刷新

试题（27）分析

资源预约协议 RSVP 是根据用户要求的服务质量，由连接的接收方（或下游结点）向中间路由器（或上游结点）预约资源。预约的资源是一种“软状态”，必须定期进行更新。

参考答案

（27）D

试题（28）

OSPF 协议使用__（28）__分组来保持与其邻居的连接。

（28）A. Hello　B. Keepalive

C. SPF（最短路径优先）　D. LSU（链路状态更新）

试题（28）分析

OSPF 的 5 种报文如表 1 所示，这些报文通过 TCP 连接传送。OSPF 路由器启动后以固定的时间间隔传播 Hello 报文，采用的目标地址 224.0.0.5 代表所有的 OSPF 路由器。在点对点网络上每 10 秒发送一次，在 NBMA 网络中每 30 秒发送一次。管理 Hello 报文交换的规则称为 Hello 协议。Hello 协议用于发现邻居，建立毗邻关系，还用于选举区域内的指定路由器 DR 和备份指定路由器 BDR。

表 1　OSPF 的 5 种报文类型

类型	报 文 类 型	功 能 描 述
1	Hello	用于发现相邻的路由器
2	数据库描述 DBD(Data Base Description)	表示发送者的链路状态数据库内容
3	链路状态请求 LSR(Link-State Request)	向对方请求链路状态信息
4	链路状态更新 LSU(Link-State Update)	向邻居路由器发送链路状态通告
5	链路状态应答 LSAck(Link-State Acknowledgement)	对链路状态更新报文的应答

参考答案

（28）A

试题（29）

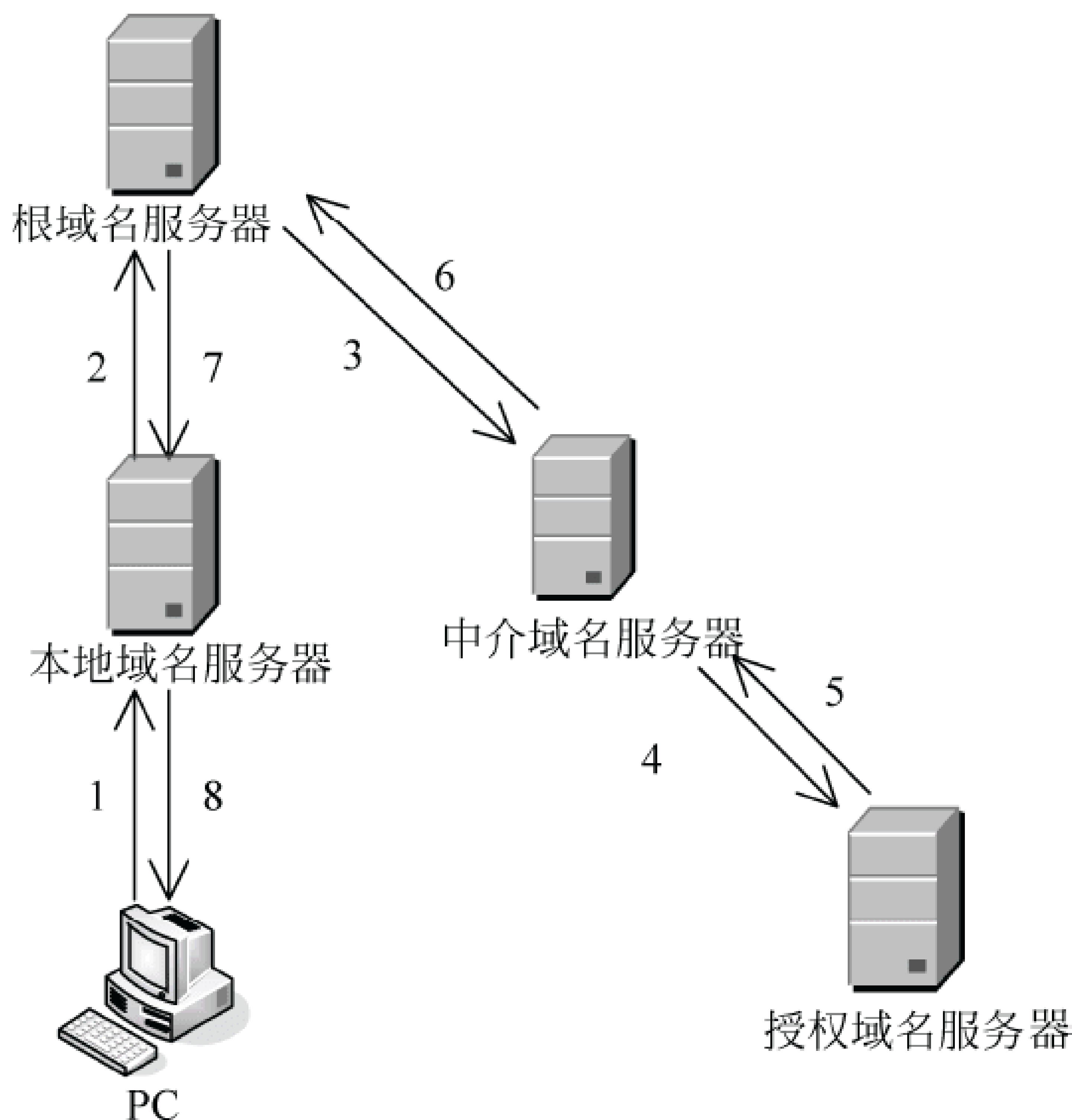
主机 PC 对某个域名进行查询，最终由该域名的授权域名服务器解析并返回结果，查询过程如下图所示。这种查询方式中不合理的是__（29）__。

（29）A. 根域名服务器采用递归查询，影响了性能

B. 根域名服务器采用迭代查询，影响了性能

C. 中介域名服务器采用迭代查询，加重了根域名服务器负担

D．中介域名服务器采用递归查询，加重了根域名服务器负担



试题（29）分析

本题考查 DNS 服务器及其原理。

DNS 查询过程分为两种查询方式：递归查询和迭代查询。

递归查询的查询方式为：当用户发出查询请求时，本地服务器要进行递归查询。这种查询方式要求服务器彻底地进行名字解析，并返回最后的结果——IP 地址或错误信息。如果查询请求在本地服务器中不能完成，那么服务器就根据它的配置向域名树中的上级服务器进行查询，在最坏的情况下可能要查询到根服务器。每次查询返回的结果如果是其他名字服务器的 IP 地址，则本地服务器要把查询请求发送给这些服务器做进一步的查询。

迭代查询的查询方式为：服务器与服务器之间的查询采用迭代的方式进行，发出查询请求的服务器得到的响应可能不是目标的 IP 地址，而是其他服务器的引用（名字和地址），那么本地服务器就要访问被引用的服务器，做进一步的查询。如此反复多次，每次都更接近目标的授权服务器，直至得到最后的结果——目标的 IP 地址或错误信息。

根域名服务器为众多请求提供域名解析，若采用递归方式会大大影响性能。

参考答案

（29）A

试题（30）、（31）

如果 DNS 服务器更新了某域名的 IP 地址，造成客户端无法访问网站，在客户端通常有两种方法解决此问题：

1．在 Windows 命令行下执行＿（30）＿命令；

2．停止系统服务中的＿（31）＿服务。

（30）A．nslookup　　B．ipconfig /renew

C．ipconfig /flushdns　　D．ipconfig /release

（31）A．SNMP　Client　　B．DNS Client

C．Plug and Play　　D．Remote Procedure Call（RPC）

试题（30）、（31）分析

本题考查 DNS 服务器及其原理。

当 DNS 服务器更新了某域名的 IP 地址后，客户端可能由于缓存中的域名记录尚未更新，无法访问网站，此时可以通过命令 ipconfig /flushdns 或停止服务 DNS Client 来更新。

参考答案

（30）C　（31）B

试题（32）

某单位采用 DHCP 进行 IP 地址自动分配，经常因获取不到地址受到用户的抱怨，网管中心决定采用 Networking Monitor 来监视客户端和服务器之间的通信。为了寻找解决问题的方法，重点要监视＿（32）＿DHCP 消息。

（32）A．DhcpDiscover　　B．DhcpOffer

C．DhcpNack　　D．DhcpAck

试题（32）分析

本题考查 DHCP 服务器及其原理。

由于用户获取不到地址，说明服务器没能正常的提供 Offer，因此需要从 DhcpNack 报文中查找原因。

参考答案

（32）C

试题（33）

网络需求分析包括网络总体需求分析、综合布线需求分析、网络可用性与可靠性分析、网络安全性需求分析，此外还需要进行＿（33）＿。

（33）A．工程造价估算　　B．工程进度安排

C．硬件设备选型　　D．IP 地址分配分析

试题（33）分析

本题考查网络需求分析。

工程造价估算是网络需求分析中的一个重要环节。

参考答案

（33）A

试题（34）

某金融网络要求网络服务系统的可用性达到 5 个 9，也就是大于 99.999%，那么每年该金融网络系统的停机时间小于__（34）__方能满足需求。

（34）A. 5 分钟　　B. 10 分钟
　　C. 60 分钟　　D. 105 分钟

试题（34）分析

本题考查网络服务系统可用性的计算方法。一年以 365 天计算，如果服务系统可用性达到 99.999%，则每年的平均无故障时间为：MTBF=0.99999×365×24×60 分钟，则每年的平均修复时间为 MTBR=(1–0.99999)×365×24×60=5.256 分钟。所以每年的停机时间必须小于 5 分钟才能满足要求。

参考答案

（34）A

试题（35）～（38）

采用可变长子网掩码可以把大的网络划分成小的子网，或者把小的网络汇聚成大的超网。假设用户 U1 有 4000 台主机，则必须给他分配__（35）__个 C 类网络，如果分配给用户 U1 的超网号为 196.25.64.0，则指定给 U1 的地址掩码为__（36）__；假设给用户 U2 分配的 C 类网络号为 196.25.16.0～196.25.31.0，则 U2 的地址掩码应为__（37）__；如果路由器收到一个目标地址为 11000100.00011001.01000011.00100001 的数据报，则该数据报应送给用户__（38）__。

（35）A. 4　　B. 8　　C. 10　　D. 16

（36）A. 255.255.255.0　　B. 255.255.250.0
　　C. 255.255.248.0　　D. 255.255.240.0

（37）A. 255.255.255.0　　B. 255.255.250.0
　　C. 255.255.248.0　　D. 255.255.240.0

（38）A. U1　　B. U2　　C. U1 或 U2　　D. 不可到达

试题（35）～（38）分析

用户 U1 有 4000 台主机，则必须给他分配 16 个 C 类网络（256×16），则指定给 U1 的地址掩码应为 255.255.240.0。

给用户 U2 分配的 C 类网络号为 196.25.16.0～196.25.31.0，其中包含 16 个 C 类网络，所以用户 U2 的地址掩码应为 255.255.240.0。

用户 U1 的网络地址 196.25.64.0/20：　**11000100.00011001.01**000000.00000000

用户 U2 的网络地址 196.25.64.0/20：　11000100.00011001.00100000.00000000

路由器收到的数据报目标地址为：　**11000100.00011001.01**000011.00100001

根据最长匹配原则，该数据报应送给用户 U1。

参考答案

（35）D　（36）D　（37）D　（38）A

试题（39）、（40）

在 IPv6 地址无状态自动配置过程中，主机首先必须自动形成一个唯一的__（39）__，然后向路由器发送__（40）__请求报文，以便获得路由器提供的地址配置信息。

（39）A．可聚集全球单播地址　　B．站点本地单播地址
　　　C．服务器本地单播地址　　D．链路本地单播地址

（40）A．Neighbor Solicitation　　B．Router Solicitation
　　　C．Router Advertisement　　D．Neighbor Discovery

试题（39）、（40）分析

在无状态自动配置过程中，主机通过两个阶段分别获得链路本地地址和可聚合全球单播地址。首先主机将其网卡 MAC 地址附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址，并发出一个 ICMPv6 邻居发现请求报文，以验证其地址的唯一性。如果请求没有得到响应，则表明主机自我配置的链路本地地址是唯一的。否则，主机将使用一个随机产生的接口 ID 组成一个新的链路本地地址。获得链路本地地址后，主机以该地址为源地址，向本地链路中所有路由器组播路由器请求（Router Solicitation）报文，路由器以一个包含可聚合全球单播地址前缀的路由器公告（Router Advertisement）报文响应。主机用从路由器得到的地址前缀加上自己的接口 ID，自动配置一个全球单播地址，这样就可以与 Internet 中的任何主机进行通信了。

参考答案

（39）D　（40）B

试题（41）

下面 ACL 语句中，准确表达“允许访问服务器 202.110.10.1 的 WWW 服务”的是__（41）__。

（41）A．access-list 101 permit any 202.110.10.1
　　　B．access-list 101 permit tcp any host 202.110.10.1 eq www
　　　C．access-list 101 deny any 202.110.10.1
　　　D．access-list 101 deny tcp any host 202.110.10.1 eq www

试题（41）分析

本题考查 ACL 语句。

正确的 ACL 语句为：access-list 101 permit tcp any host 202.110.10.1 eq www。

参考答案

（41）B

试题（42）

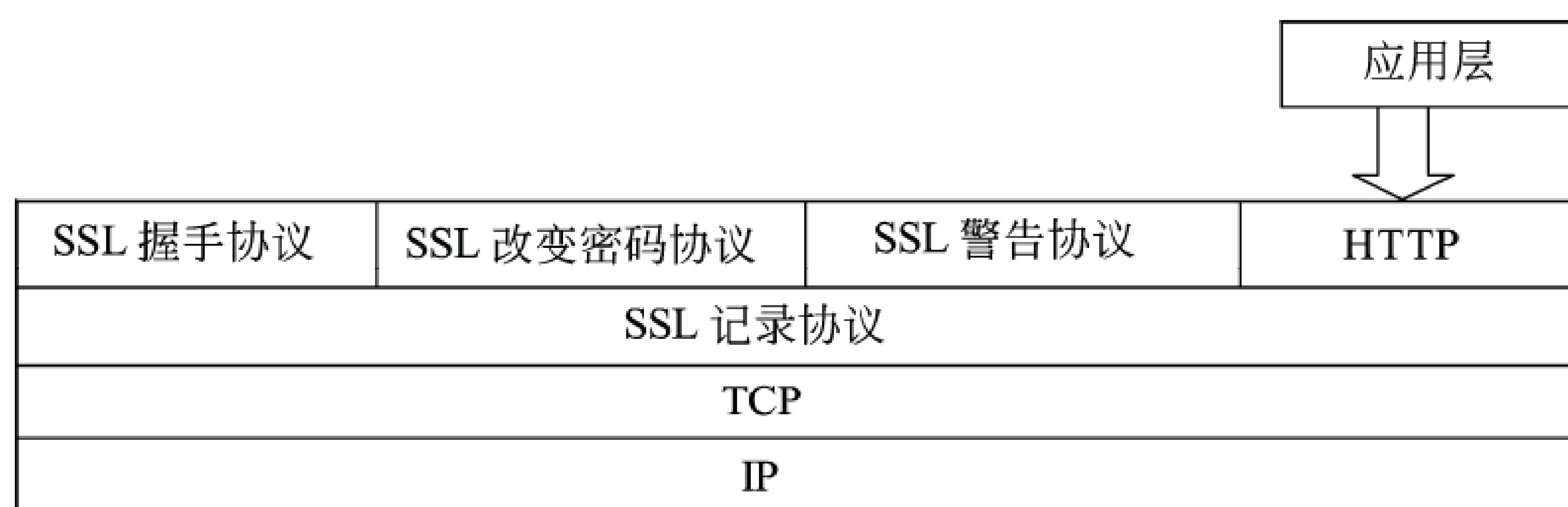
SSL 协议共有上下两层组成，处于下层的是__（42）__。

（42）A．SSL 握手协议（SSL Handshake protocol）
B．改变加密约定协议（Change Cipher spec protocol）
C．报警协议（Alert protocol）
D．SSL 记录协议（SSL Record Protocol）

试题（42）分析

本试题考查 SSL 协议及组成。

SSL 协议分为两层，底层是 SSL 记录协议，运行在传输层协议 TCP 之上，用于封装各种上层协议。一种被封装的上层协议是 SSL 握手协议，由服务器和客户端用来进行身份认证，并且协商通信中使用的加密算法和密钥。SSL 协议栈如下图所示。



参考答案

（42）D

试题（43）

ISO 7498-2 标准规定的五大安全服务是＿（43）＿。

（43）A．鉴别服务、数字证书、数据完整性、数据保密性、抗抵赖性
B．鉴别服务、访问控制、数据完整性、数据保密性、抗抵赖性
C．鉴别服务、访问控制、数据完整性、数据保密性、计费服务
D．鉴别服务、数字证书、数据完整性、数据保密性、计费服务

试题（43）分析

本试题考查 ISO 7498-2 标准。

ISO 7498-2 标准中描述了开放系统互联安全的体系结构，提出设计安全的信息系统的基础架构中应该包含 5 种安全服务（安全功能）、能够对这 5 种安全服务提供支持的 8 类安全机制和普遍安全机制，以及需要进行的 5 种 OSI 安全管理方式。其中 5 种安全服务为：鉴别服务、访问控制、数据完整性、数据保密性、抗抵赖性；8 类安全机制：加密、数字签名、访问控制、数据完整性、数据交换、业务流填充、路由控制、公证。

参考答案

（43）B

试题（44）

下面关于第三方认证服务说法中，正确的是＿（44）＿。

（44）A．Kerberos 认证服务中保存数字证书的服务器叫 CA

B．第三方认证服务的两种体制分别是 Kerberos 和 PKI

C．PKI 体制中保存数字证书的服务器叫 KDC

D．Kerberos 的中文全称是“公钥基础设施”

试题（44）分析

本题考查认证服务。

Kerberos 可以防止偷听和重放攻击，保护数据的完整性。Kerberos 的安全机制如下。

- AS（Authentication Server）：认证服务器，是为用户发放 TGT 的服务器。
- TGS（Ticket Granting Server）：票证授予服务器，负责发放访问应用服务器时需要的票证。认证服务器和票据授予服务器组成密钥分发中心（Key Distribution Center，KDC）。
- V：用户请求访问的应用服务器。
- TGT（Ticket Granting Ticket）：用户向 TGS 证明自己身份的初始票据，即 $K_{TGS}(A,K_S)$。

公钥基础结构（Public Key Infrastructure，PKI）是运用公钥的概念和技术来提供安全服务的、普遍适用的网络安全基础设施，包括由 PKI 策略、软硬件系统、认证中心、注册机构（Registration Authority，RA）、证书签发系统和 PKI 应用等构成的安全体系。

参考答案

（44）B

试题（45）

下面安全协议中，IP 层安全协议是__（45）__。

（45）A．IPSec　　B．L2TP　　C．TLS　　D．PPTP

试题（45）分析

本题考查安全协议的工作层次。

IPSec、L2TP、PPTP 均是隧道协议，其中 L2TP、PPTP 工作在数据链路层，IPSec 工作在 IP 层；TLS 是传输层安全协议。

参考答案

（45）A

试题（46）

采用 Kerberos 系统进行认证时，可以在报文中加入__（46）__来防止重放攻击。

（46）A．会话密钥　　B．时间戳　　C．用户 ID　　D．私有密钥

试题（46）分析

本题考查 Kerberos 系统认证。

时间戳可用来进行防重放攻击。

参考答案

（46）B

试题（47）

某单位建设一个网络，设计人员在经过充分的需求分析工作后，完成了网络的基本设计。但是，由于资金受限，网络建设成本超出预算，此时，设计人员正确的做法是 （47） 。

（47）A．为符合预算，推翻原设计，降低网络设计标准重新设计

B．劝说该单位追加预算，完成网络建设

C．将网络建设划分为多个周期，根据当前预算，设计完成当前周期的建设目标

D．保持原有设计，为符合预算降低设备性能，采购低端设备

试题（47）分析

本题考查网络的需求分析与设计。

若网络建设成本超出预算，需根据当前预算，设计完成当前周期的建设目标。

参考答案

（47）C

试题（48）～（50）

某数据中心根据需要添加新的数据库服务器。按照需求分析，该数据库服务器要求具有高速串行运算能力，同时为了该服务器的安全，拟选用 Unix 操作系统。根据以上情况分析，该服务器应选择 （48） 架构的服务器。其中 （49） 系列的 CPU 符合该架构。若选用了该 CPU，则采用 （50） 操作系统是合适的。

（48）A．RISC　　B．CISC　　C．IA-32　　D．VLIW

（49）A．Opteron　　B．Xeon　　C．Itanium　　D．Power

（50）A．HP-UX　　B．Solaris　　C．AIX　　D．A/UX

试题（48）～（50）分析

本题考查服务器的基础知识。

按服务器的处理器架构（即服务器 CPU 所采用的指令系统）可把服务器划分为 RISC 架构服务器和 IA 架构服务器。后者包括 CISC 架构服务器和 VLIW 架构服务器两种。

其中 RISC 的指令系统相对简单，它只要求硬件执行很有限且最常用的那部分指令，大部分复杂的操作则使用成熟的编译技术，由简单指令合成。目前在中高档服务器特别是高档服务器普遍采用 RISC 指令系统的 CPU。

配备 RISC 架构 CPU 的服务器一般采用 Unix 操作系统，其具备高速运算能力，并且由于使用 Unix 操作系统，其安全性、可靠性较高。

根据题目要求需要选择数据库服务器，数据库服务器对于处理器性能要求很高。数据库服务器需要根据需求进行查询，然后将结果反馈给用户。如果查询请求非常多，比如大量用户同时查询的时候，如果服务器的处理能力不够强，无法处理大量的查询请求并做出应答。同时为了数据库服务器的安全，拟选用 Unix 操作系统，所以此时应选取

RISC 架构服务器。

IBM 公司的 Power 系列处理器是 RISC 处理器芯片， Opteron（皓龙）是美国 AMD 公司生产基于 x86-64 架构的 CPU，Xeon 则是 Intel 公司的 X86 架构的 CPU，而 Itanium（官方中文名称为安腾），是 Intel Itanium 架构（通常称之为 IA-64）的 64 位处理器。根据问题（48）可以判定，此处应选择 Power 系列的 CPU。

由于确定采用 IBM 公司的 Power 系列处理器，所以操作系统的选取就应该为 AIX。这是因为 RISC 架构服务器采用的主要是封闭的发展策略，即由单个厂商提供垂直的解决方案，从服务器的系统硬件到系统软件都由这个厂商完成。AIX 是 IBM 开发的一套 Unix 操作系统，其全面支持 IBM 公司的 Power 系列处理器；HP-UX 全称为 Hewlett Packard UniX，是惠普 9000 系列服务器的操作系统，可以在 HP 的 PA-RISC 处理器、Intel 的 Itanium 处理器的电脑上运行；Solaris 是 Sun Microsystems 研发的 Unix 操作系统操作系统，其支持多种系统架构：SPARC，x86 and x64；A/UX（Apple Unix）是苹果电脑（Apple Computer）公司所开发的 UNIX 操作系统，此操作系统可以在该公司的一些麦金塔电脑（Macintosh）上运行。

参考答案

（48）A　（49）D　（50）C

试题（51）

网络安全设计是网络规划与设计中的重点环节，以下关于网络安全设计原则的说法，错误的是__（51）__。

（51）A. 网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提

B. 强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失

C. 考虑安全问题解决方案时无需考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合

D. 充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件

试题（51）分析

本题考查网络安全设计。

网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提；强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失；考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合；充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件。

参考答案

（51）C

试题（52）～（54）

某财务部门需建立财务专网，A 公司的李工负责对该网络工程项目进行逻辑设计，他调研后得到的具体需求如下：

① 用户计算机数量 40 台，分布在二层楼内，最远距离约 60 米；

② 一共部署 7 个轻负载应用系统，其中 5 个系统不需要 Internet 访问，2 个系统需要 Internet 访问；

李工据此给出了设计方案，主要内容可概述为：

① 出口采用核心交换机+防火墙板卡设备组成财务专网出口防火墙，并通过防火墙策略将需要 Internet 访问的服务器进行地址映射；

② 财务专网使用 WLAN 为主，报账大厅用户、本财务部门负责人均可以访问财务专网和 Internet；

③ 采用 3 台高性能服务器部署 5 个不需要 Internet 访问的应用系统，1 台高性能服务器部署 2 个需要 Internet 访问的应用系统。

针对用户访问，你的评价是<u>（52）</u>。

针对局域网的选型，你的评价是<u>（53）</u>。

针对服务器区的部署，你的评价是<u>（54）</u>。

（52）A．用户权限设置合理

B．不恰当，报账大厅用户不允许访问 Internet

C．不恰当，财务部门负责人不允许访问 Internet

D．不恰当，财务部门负责人不允许访问财务专网

（53）A．选型恰当

B．不恰当，WLAN 成本太高

C．不恰当，WLAN 不能满足物理安全要求

D．不恰当，WLAN 不能满足覆盖范围的要求

（54）A．部署合理

B．不恰当，7 个业务系统必须部署在 7 台物理服务器上

C．不恰当，没有备份服务器，不能保证数据的安全性和完整性

D．不恰当，所有服务器均需通过防火墙策略进行地址映射

试题（52）～（54）分析

本题考查逻辑网络设计、物理网络设计的相关知识。

从用户的主要需求可以看出，覆盖范围最远距离未超出 90 米，可以覆盖；

财务专网是安全级别比较高的财务部门内部网络，如果采用 WLAN 为主，不能满足物理安全要求，要求一般财务人员只能访问财务专网进行办公，不能访问 Internet。

业务系统最好按照允许访问对象划分部署，通过防火墙进行安全防火和地址转换，但是业务系统中数据非常重要，所以必须有备份服务器来保证数据的安全性和完整性。

参考答案

（52）B　（53）C　（54）C

试题（55）

按照 IEEE 802.3 标准，以太帧的最大传输效率为__（55）__。

（55）A. 50%　　B. 87.5%　　C. 90.5%　　D. 98.8%

试题（55）分析

本题考查以太帧的基础知识。

按照 IEEE 802.3 标准，标准以太帧的最大 MTU 值为 1500Bytes，而在以太帧中头标记和 CRC（Cyclic Redundancy Check）共有 18Bytes，所以其最大传输效率 1500/1518=98.8%。

参考答案

（55）D

试题（56）

以下关于层次化网络设计原则的叙述中，错误的是__（56）__。

（56）A. 层次化网络设计时，一般分为核心层、汇聚层、接入层三个层次
　　B. 应当首先设计核心层，再根据必要的分析完成其他层次设计
　　C. 为了保证网络的层次性，不能在设计中随意加入额外连接
　　D. 除去接入层，其他层次应尽量采用模块化方式，模块间的边界应非常清晰

试题（56）分析

本题考查层次化网络设计原则的基础知识。

层次化网络设计应该遵循一些简单的原则，这些原则可以保证设计出来的网络更加具有层次的特性：

① 在设计时，设计者应该尽量控制层次化的程度，一般情况下，由核心层、汇聚层、接入层三个层次就足够了，过多的层次会导致整体网络性能的下降，并且会提高网络的延迟，同时也方便网络故障排查和文档编写。

② 在接入层应当保持对网络结构的严格控制，接入层的用户总是为了获得更大的外部网络访问带宽，而随意申请其他的渠道访问外部网络，这是不允许的。

③ 为了保证网络的层次性，不能在设计中随意加入额外连接，额外连接是指打破层次性，在不相邻层次间的连接，这些连接会导致网络中的各种问题，例如缺乏汇聚层的访问控制和数据报过滤等。

④ 在进行设计时，应当首先设计接入层，根据流量负载、流量和行为的分析，对上层进行更精细得容量规划，再依次完成各上层的设计。

⑤ 除去接入层的其他层次，应尽量采用模块化方式，每个层次由多个模块或者设备集合构成，每个模块间的边界应非常清晰。

参考答案

（56）B

试题（57）

在以下各种网络应用中，节点既作为客户端同时又作为服务端的是__（57）__。

（57）A．P2P 下载
B．B/S 中应用服务器与客户机之间的通信
C．视频点播服务
D．基于 SNMP 协议的网管服务

试题（57）分析

本题考查网络应用的基础知识。

B/S 中应用服务器与客户机之间的通信、视频点播服务和基于 SNMP 协议的网管服务在工作是基于 Client/Server 和 Browse/Server 模式，这些模式的特点是：它们都是以应用为核心的，在网络中必须有应用服务器，用户的请求必须通过应用服务器完成。而 P2P 下载服务是对等网络结构，网上各台节点有相同的功能，无主从之分，一个节点都是既可作为服务器，又可以作为工作站。

参考答案

（57）A

试题（58）

在 OSPF 中，路由域存在骨干域和非骨干域，某网络自治区域中共有 10 个路由域，其区域 id 为 0～9，其中__（58）__为骨干域。

（58）A．Area 0　B．Area 1　C．Area 5　D．Area 9

试题（58）分析

本题考查 OSPF 的基础知识。

在 OSPF 中，采用分区域计算，将网络中所有 OSPF 路由器划分成不同的区域，每个区域负责各自区域精确的 LSA 传递与路由计算，然后再将一个区域的 LSA 简化和汇总之后转发到另外一个区域。区域的命名可以采用整数数字，如 1、2、3、4，也可以采用 IP 地址的形式，0.0.0.1、0.0.0.2，因为采用了 Hub-Spoke 的架构，所以必须定义出一个核心，然后其他部分都与核心相连，OSPF 的区域 0 就是所有区域的核心，称为 BackBone 区域（骨干区域），而其他区域称为 Normal 区域（常规区域）。

参考答案

（58）A

试题（59）

测试工具应在交换机发送端口产生__（59）__线速流量来进行链路传输速率测试。

（59）A．100%　B．80%　C．60%　D．50%

试题（59）分析

本题考查网络系统测试过程中，针对交换机发送端口进行链路传输速率测试的标准。

在交换机发送端口产生 100%满线速流量，在 HUB 发送端口产生 50%线速流量。

参考答案

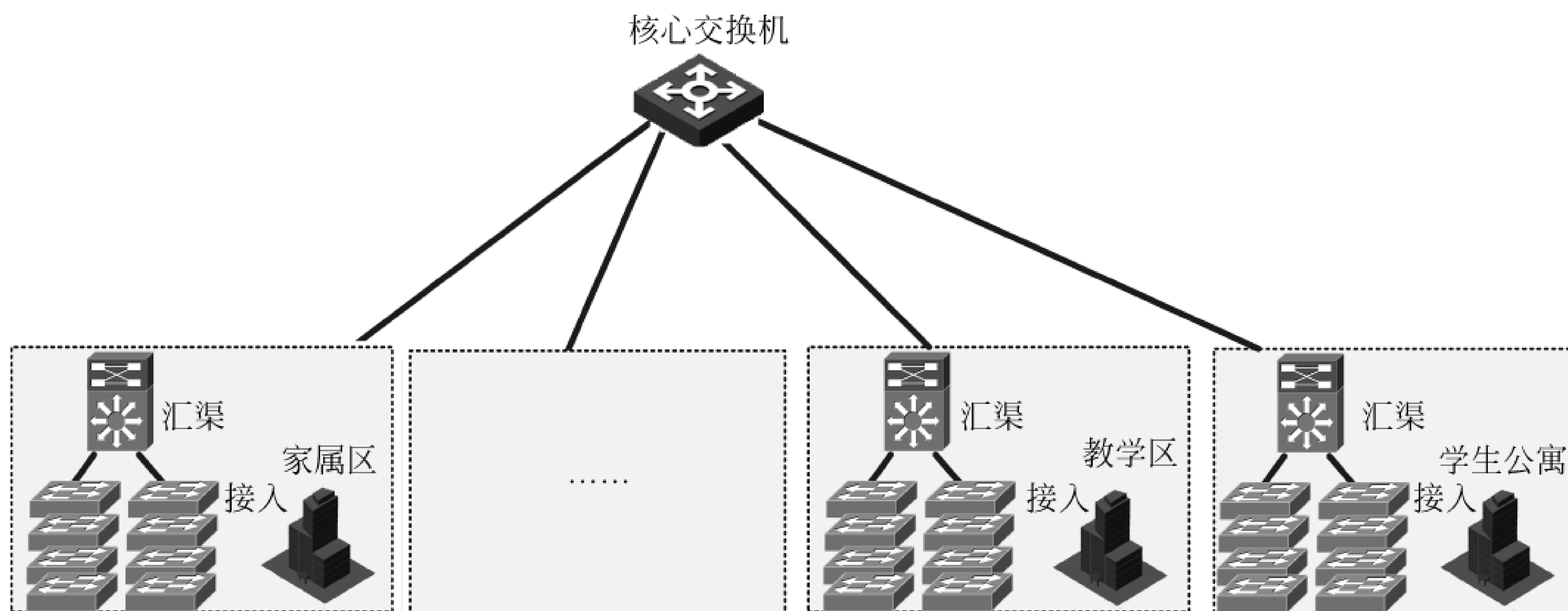
（59）A

试题（60）、（61）

某高校的校园网由 1 台核心设备、6 台汇聚设备、200 台接入设备组成，网络拓扑结构如下图所示，所有汇聚设备均直接上联到核心设备，所有接入设备均直接上联到汇聚设备，在网络系统抽样测试中，按照抽样规则，最少应该测试__（60）__条汇聚层到核心层的上联链路和__（61）__条接入层到汇聚层的上联链路。

（60）A．3　　B．4　　C．5　　D．6

（61）A．20　　B．30　　C．40　　D．50



试题（60）、（61）分析

本题考查网络系统抽样测试中的抽样规则：对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10%的比例进行抽样测试，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

该网络中汇聚层到核心层一共 6 条上联链路，接入层到汇聚层一共 200 条上联链路。根据该抽样规则，则一共应测试 6 条汇聚层到核心层上联链路，20 条接入层到汇聚层的上联链路。

参考答案

（60）D　（61）A

试题（62）

某公司主营证券与期货业务，有多个办公网点，要求企业内部用户能够高速地访问企业服务器，并且对网络的可靠性要求很高。工程师给出设计方案：

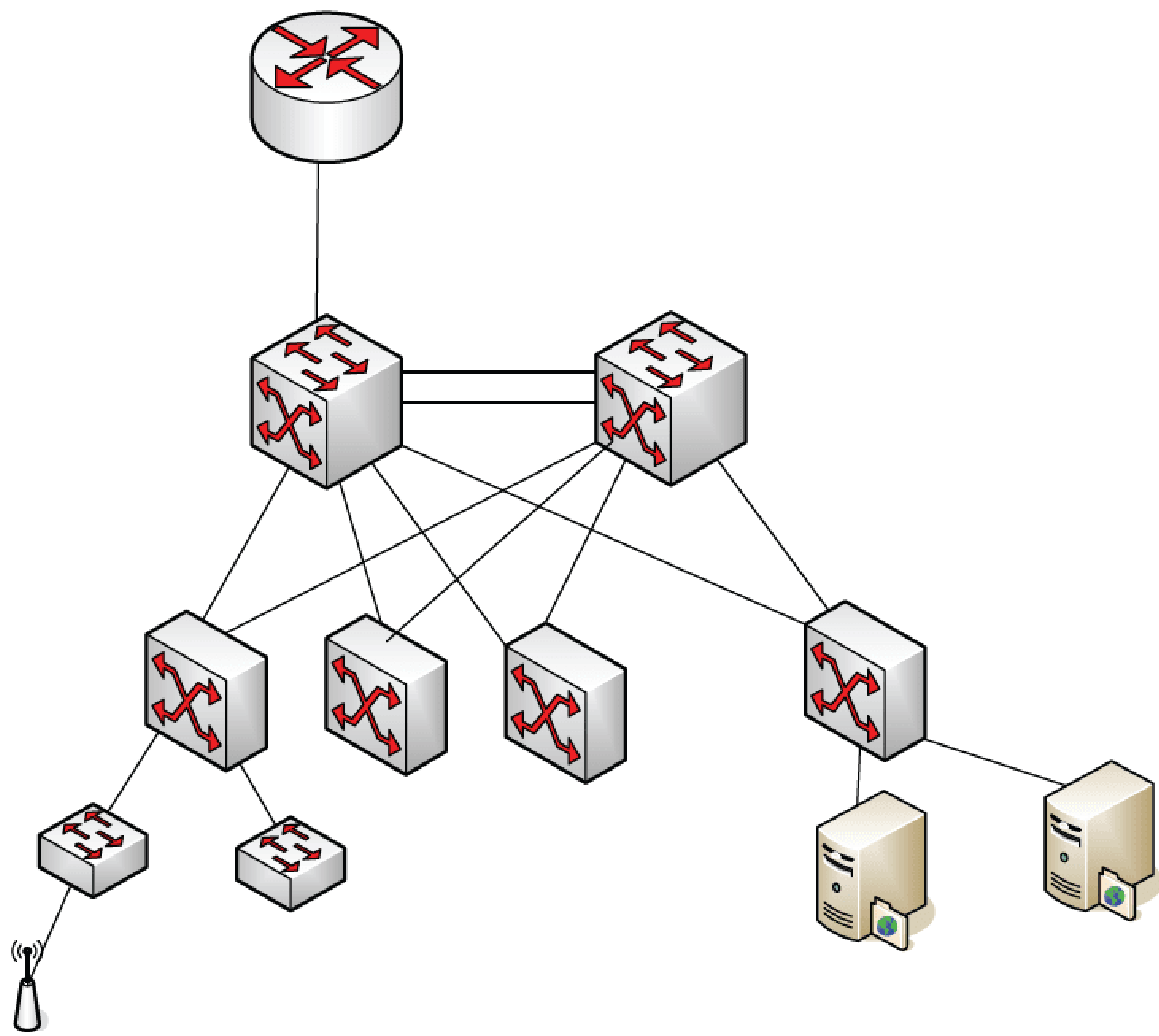
① 采用核心层、汇聚层、接入层三层结构；

② 骨干网使用千兆以太网；

③ 为了不改变已有建筑的结构，部分网点采用 WLAN 组网；

④ 根据企业需求，将网络拓扑结构设计为双核心来进行负载均衡，当其中一个核心交换机出现故障时，数据能够转换到另一台交换机上，起到冗余备份的作用。

网络拓扑如下图所示。



针对网络的拓扑设计，你的评价是__（62）__。

（62）A. 恰当合理

B. 不恰当，两个核心交换机都应直接上联到路由器上，保证网络的可靠性

C. 不恰当，为保证高速交换，接入层应使用三层交换机

D. 不恰当，为保证核心层高速交换，服务器应放在接入层

试题（62）分析

本题考查网络规划与设计。

两个核心交换机都应直接上联到路由器上，采用冗余连接保证网络的可靠性；接入层只是保障用户接入，无需三层交换机；服务器放在接入层印象访问速度。

参考答案

（62）B

试题（63）

一台 CISCO 交换机和一台 H3C 交换机相连，互联端口都工作在 VLAN TRUNK 模式下，这两个端口应该使用的 VLAN 协议分别是__（63）__。

（63）A．ISL 和 IEEE 802.10　　B．ISL 和 ISL

C．ISL 和 IEEE 802.1Q　　D．IEEE 802.1Q 和 IEEE 802.1Q

试题（63）分析

本题考查 VLAN TRUNK 的基本知识。

在交换设备之间实现 VLAN TRUNK 功能，必须遵守相同的 VLAN 协议标准。

目前，在交换设备中常用的 VLAN 协议有 ISL（Cisco 公司内部交换链路协议）、IEEE 802.10（原为 FDDI 的安全标准协议）和国际标准 IEEE 802.1Q。其中，ISL（Inter-Switch Link）是 Cisco 交换机内部链路的一个 VLAN 协议，它是个私有协议，仅适用于 Cisco 设备。IEEE 802.10 的正式名称是 IEEE 802.10 Interoperable LAN/MAN Security Standard，是一个 OSI 第二层的协议，包括了验证（Authentication）和加密（Encryption）等机制。其目的是在数据链路层内安全地交换数据，为此它定义了称为安全数据互换（SDE：Secure Data Exchange）的协议数据单元（PDU）。虽然 802.10 确实是一个标准，但它毕竟只是一个安全性标准，并不能完全满足虚拟网的需要，而且目前对 802.10 报头中域的使用，各厂家仍是各自为政，互不兼容。IEEE 802.1Q 标准提供了对 VLAN 明确的定义及其在交换式网络中的应用。该标准的发布，确保了不同厂商产品的互操作能力，并在业界获得了广泛的推广。它成为 VLAN 发展史上的里程碑。IEEE 802.1Q 的出现打破了 VLAN 依赖于单一厂商的僵局，从一个侧面推动了 VLAN 的迅速发展。因此，在不同厂家交换机互连要实现 VLAN TRUNK 功能时，必须在直接相连的两台交换机端口都封装 IEEE 802.1Q 协议，从而保证协议的一致性，否则不能正确地传输多个 VLAN 信息。

参考答案

（63）D

试题（64）、（65）

在进行无线 WLAN 网络建设时，现在经常使用的协议是 IEEE 802.11b/g/n，采用的共同工作频带为__（64）__。其中为了防止无线信号之间的干扰，IEEE 将频段分为 13 个信道，其中仅有三个信道是完全不覆盖的，它们分别是__（65）__。

（64）A．2.4 GHz　　B．5 GHz　　C．1.5 GHz　　D．10 GHz

（65）A．信道 1、6 和 13　　B．信道 1、7 和 11

C．信道 1、7 和 13　　D．信道 1、6 和 11

试题（64）、（65）分析

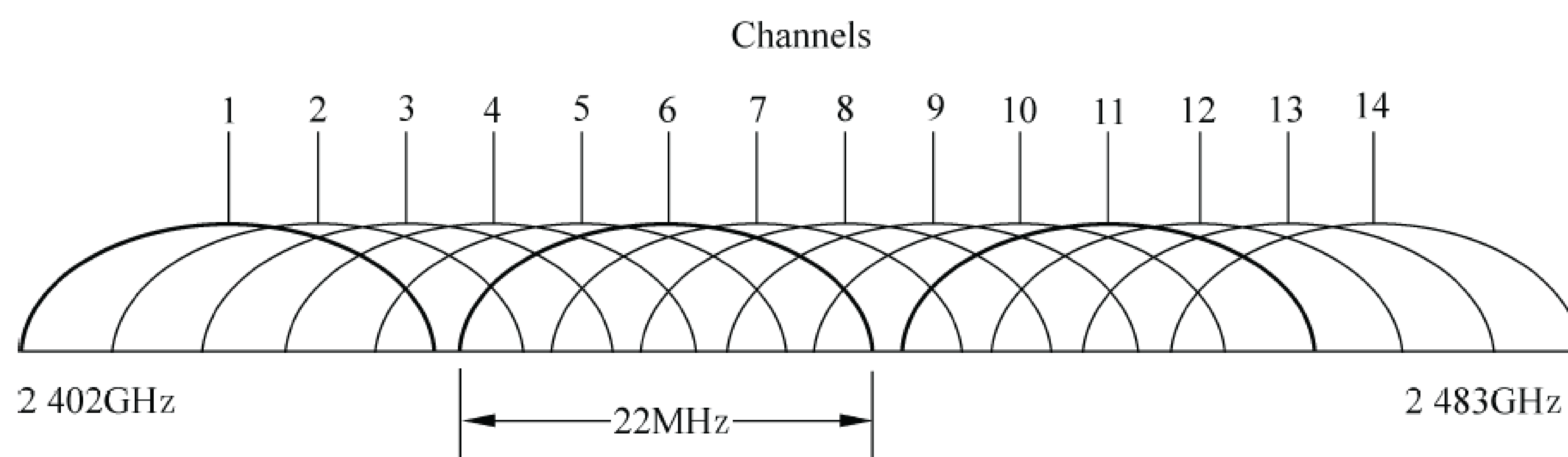
本题考查 WLAN 的有关基本知识。

802.11 是 IEEE 最初制定的一个无线局域网标准，主要用于解决网络用户与用户终端的无线接入；其中 802.11a 工作在 5.4G 频段、最高速率 54 兆、主要用在远距离的无线连接；802.11b 工作在 2.4G 频段、最高速率 11 兆、目前已经逐步被淘汰；802.11g 工作在 2.4G 频段、最高速率 54 兆；802.11n 工作在 2.4GHz 或者 5GHz、最高速率可达 600 兆。因此 IEEE 802.11b/g/n，采用的共同工作频带为 2.4GHz。

目前主流的无线 WIFI 网络设备不管是 802.11b/g 还是 802.11b/g/n 一般都支持 13 个信道。它们的中心频率虽然不同，但是因为都占据一定的频率范围，所以会有一些相互重叠的情况。信道也称作通道（Channel）、频段，是以无线信号（电磁波）作为传输载体的数据信号传送通道。无线网络（路由器、AP 热点、电脑无线网卡）可在多个信道上运行。在无线信号覆盖范围内的各种无线网络设备应该尽量使用不同的信道，以避免信号之间的干扰。

下表是常用的 2.4GHz（=2400MHz）频带的信道划分。实际一共有 14 个信道（图中画出了第 14 信道），但第 14 信道一般不用。表中列出的是信道的中心频率。每个信道的有效宽度是 20MHz，另外还有 2MHz 的强制隔离频带。即对于中心频率为 2412 MHz 的 1 信道，其频率范围为 2401～2423MHz。

信道	中心频率	信道	中心频率	信道	中心频率
1	2412MHz	2	2417MHz	3	2422MHz
4	2427MHz	5	2432MHz	6	2437MHz
7	2442MHz	8	2447MHz	9	2452MHz
10	2457MHz	11	2462MHz	12	2467MHz
13	2472MHz				



从上图中很容易看到其中 1、6、11 这三个信道（红色标记）之间是完全没有交叠的，也就是三个不互相重叠的信道，每个信道 20MHz 带宽。图中也很容易看清楚其他各信道之间频谱重叠的情况。另外，如果设备支持，除 1、6、11 三个一组互不干扰的信道外，还有 2、7、12；3、8、13；4、9、14 三组互不干扰的信道。

参考答案

（64）A （65）D

试题（66）

在网络数据传输过程中都是收、发双向进行的。一般来说，对于光纤介质也就需要两条光纤分别负责数据的发送和接受。近年来已经有了在单条光纤上同时传输收发数据的技术，下面支持单条光纤上同时传输收发数据的技术是（66）。

（66）A．WiFi 和 WiMAX　　B．ADSL 和 VDSL
C．PPPoE 和 802.1x　　D．GPON 和 EPON

试题（66）分析

无源光网络（Passive Optical Network，PON）是一种纯介质网络，PON 目前主要有 GPON（ITU 协议）和 EPON（IEEE 协议）两种协议技术。

通过 PON，单根光纤从服务提供商的设备延伸到靠近居民区或商务中心的位置。“无源”是指该系统在服务提供商和客户之间不需要电源和有源的电子组件。它仅由光纤、分路器、接头和连接器组成。一根光纤可为多个客户提供服务，而此前的系统要求每个客户都有独立的光纤，这样就大大节省了光纤资源。

参考答案

（66）D

试题（67）

光缆布线工程结束后进行测试是工程验收的关键环节。以下指标中不属于光缆系统的测试指标的是（67）。

（67）A．最大衰减限值　　B．回波损耗限值
C．近端串扰　　D．波长窗口参数

试题（67）分析

本题主要考察光缆布线工程中对光缆系统的测试指标。其中近端串扰（Near End Cross-Talk（NEXT））是指在 UTP 电缆链路中一对线与另一对线之间的因信号耦合效应而产生的串扰，是对性能评价的最主要指标，近端串扰用分贝（dB）来度量，不属于光缆系统的测试指标。

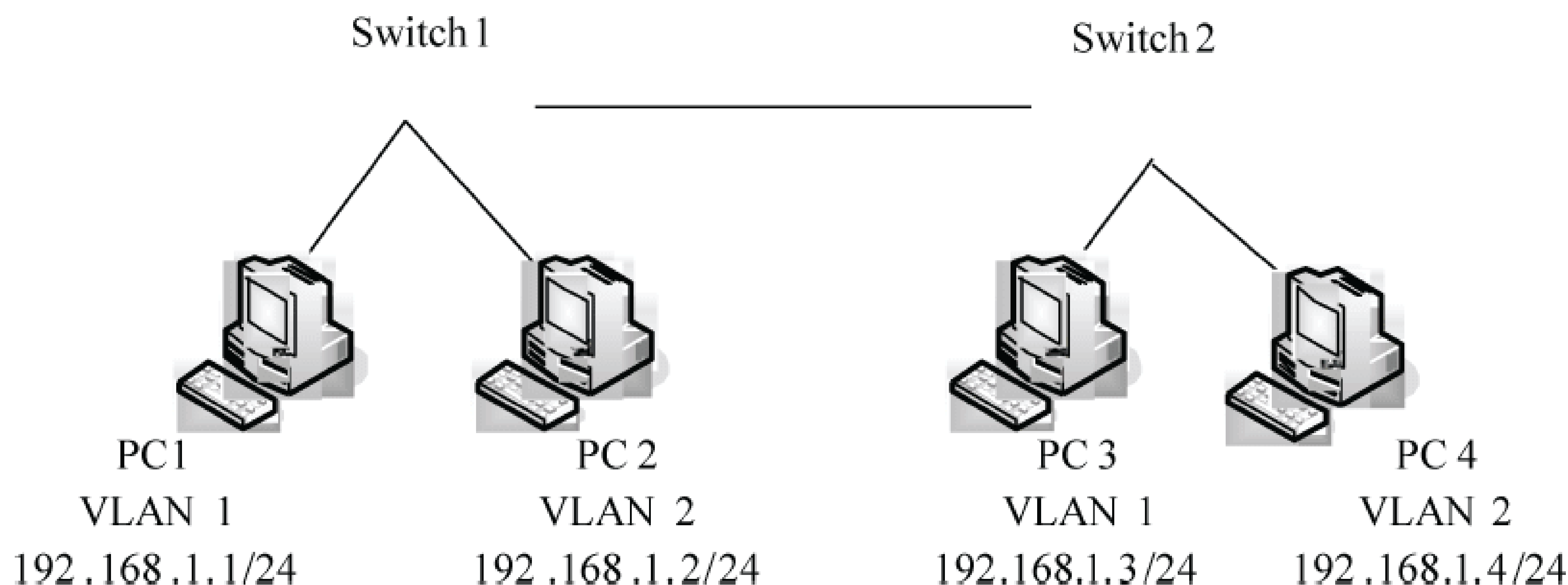
参考答案

（67）C

试题（68）、（69）

如图所示网络结构，当 Switch 1 和 Switch 2 都采用默认配置，那么 PC2 和 PC4 之间不能通信，其最可能的原因是（68）。如果要解决此问题，最快捷的解决方法是（69）。

（68）A．PC2 和 PC4 的 IP 地址被交换机禁止通过
B．PC2 和 PC4 的 VLAN 被交换机禁止通过
C．PC2 和 PC4 的 MAC 地址被交换机禁止通过
D．PC2 和 PC4 的接入端口被交换机配置为 down



（69）A．把 Switch 1 和 Switch 2 连接端口配置为 trunk 模式
B．把 Switch 1 和 Switch 2 连接端口配置为 access 模式
C．把 Switch 1 和 Switch 2 设备配置为服务器模式
D．把 Switch 1 和 Switch 2 设备配置为客户端模式

试题（68）、（69）分析

本题考查交换机基本配置的相关知识。

根据题意及图中所示，Switch 1 和 Switch 2 采用默认配置，则 IP 地址、MAC 地址都不会被禁止，端口也为激活状态。在没有配置 VLAN 之前，由交换机互连的网络默认同属于 VLAN1。VLAN1 也是默认的本征 VLAN。本征 VLAN 是指交换机允许默认传输信息的 VLAN。对于不是本征 VLAN 的其他 VLAN 默认是不允许在交换机之间传输信息的。

PC2 和 PC4 的 IP 地址为同一网段，也属于同一 VLAN（VLAN2）。PC2 和 PC4 之间不能通信的原因可能是 Switch 1 和 Switch 2 的连接端口不允许除本征 VLAN 之外的其他 VLAN（VLAN2）通过，默认情况下 Switch 1 和 Switch 2 连接端口为 access 模式，因此，要解决此问题，最快捷的解决方法是把 Switch 1 和 Switch 2 连接端口配置为 trunk 模式，该模式下允许多个不同的 VLAN 通过。

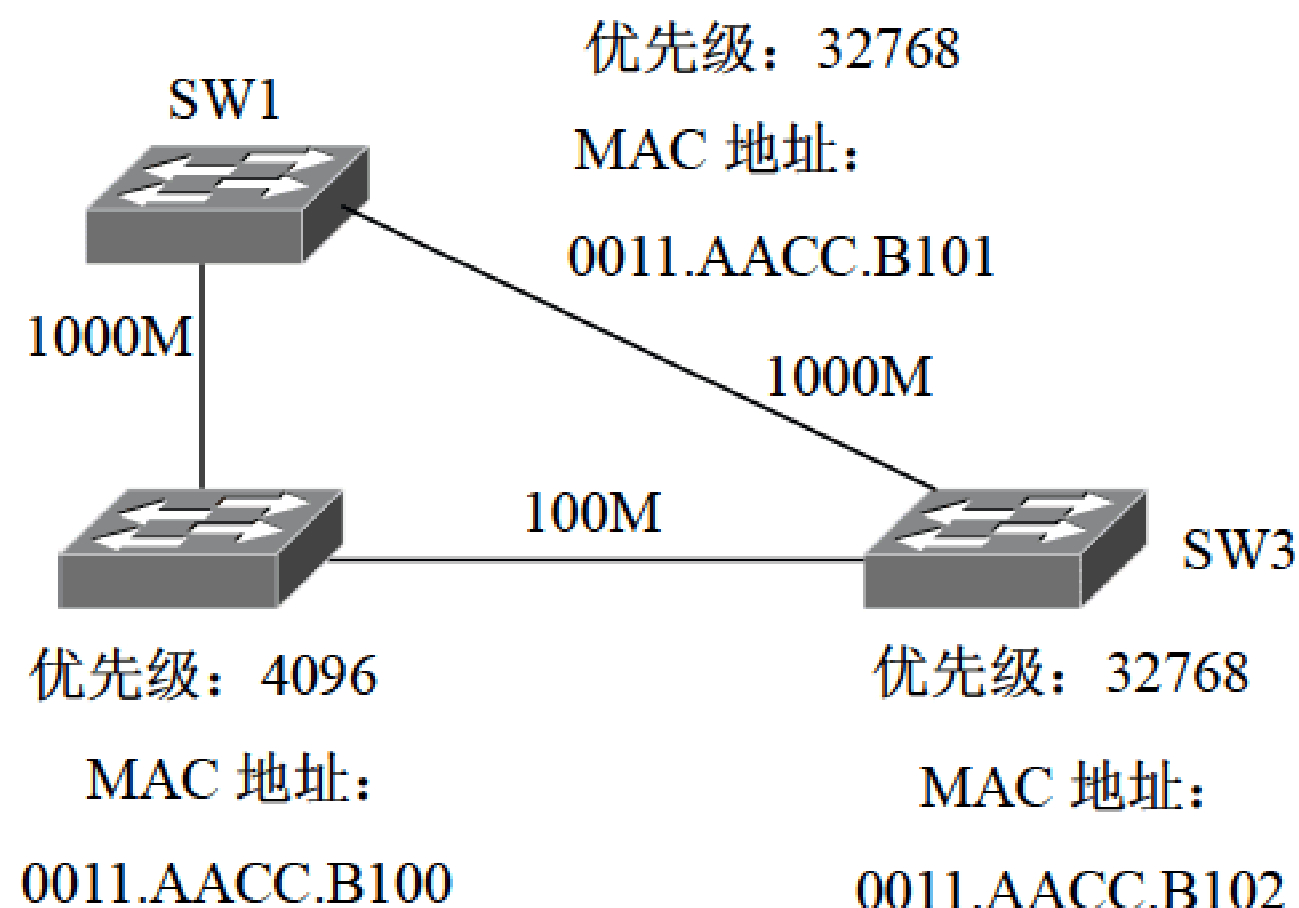
参考答案

（68）B　（69）A

试题（70）

在 STP 生成树中，断开的链路并不是随意选择的，而是通过设备、接口、链路优先级等决定的。在下图所示的连接方式中，哪条链路是作为逻辑链路断开而备份使用的？__（70）__。

（70）A．SW1 和 SW2 之间的链路
B．SW1 和 SW3 之间的链路
C．SW2 和 SW3 之间的链路
D．任意断开一条皆可



试题（70）分析

本题考查 STP 生成树的有关知识。在 STP 生成树中，断开的链路并不是随意选择的，而是通过设备、接口、链路优先级等决定的。具体的原则为：首先在局域网中找一台设备为根桥，根桥由桥 ID 的大小决定，桥 ID 值最小的设备为根桥。桥 ID=桥优先级+桥 MAC 地址，其中“桥”就是“网桥”，即交换机。默认情况下交换机的优先级都是 32768，如果需要某一台设备为根桥的话，直接将其优先级改小即可，不过交换机的优先级规定必须为 4096 的倍数。

如图所示，SW2 是根桥，SW3 到 SW2 有两条路径，要根据两条链路的成本值决定应该逻辑断开哪一条。其中 SW2 和 SW3 的优先级相同，又根据链路带宽成本，其中 100M 的路径成本为 19，1000M 的路径成本为 4。所以 SW2-SW3 的直连链路成本为 19，SW3-SW1-SW2 的链路成本为 8，所以应该断开 SW2-SW3 之间的逻辑链路，备份使用。

参考答案

（70）C

试题（71）～（75）

The API changes should provide both source and binary __（71）__ for programs written to the original API. That is, existing program binaries should continue to operate when run on a system supporting the new API. In addition, existing __（72）__ that are re-compiled and run on a system supporting the new API should continue to operate. Simply put, the API __（73）__ for multicast receivers that specify source filters should not break existing programs. The changes to the API should be as small as possible in order to simplify the task of converting existing __（74）__ receiver applications to use source filters. Applications should be able to detect when the new __（75）__ filter APIs are unavailable (e.g., calls fail with the ENOTSUPP error) and react gracefully (e.g., revert to old non-source-filter API or display a meaningful error message to the user).

（71）A. capability　　B. compatibility　　C. labiality　　D. reliability

（72）A. systems　　B. programs　　C. applications　　D. users

（73）A. connections　　B. changes　　C. resources　　D. considerations

（74）A．multicast B．unicast C．broadcast D．anycast

（75）A．resource B．state C．destination D．source

参考译文

对于 API 的改变应该与用原来 API 编写的程序的源代码和二进制代码兼容。亦即，原有程序的二进制代码应该可以运行在支持新 API 的系统上。此外，现有的应用经过重新编译，也可以运行在支持新 API 的系统上。简言之，对于说明了源过滤的组播接收器，API 的改变不能破坏现有的程序。API 的改变应该尽量小，以便简化转换现有的使用源过滤的组播接收器应用的工作。当新的源过滤 API 不可用时，应用程序应该能够检测到（例如调用失败，出现 ENOTSUPP 错误），并且给出温和的反应（例如转向老的非源过滤 API，或者向用户显示有用的错误信息）。

参考答案

（71）B （72）C （73）B （74）A （75）D

第 17 章　2013 下半年网络规划设计师下午试卷 I 试题分析与解答

试题一（共 25 分）

阅读以下关于某园区企业网络的叙述，回答问题 1 至问题 4。

企业网络拓扑结构如图 1-1 所示。

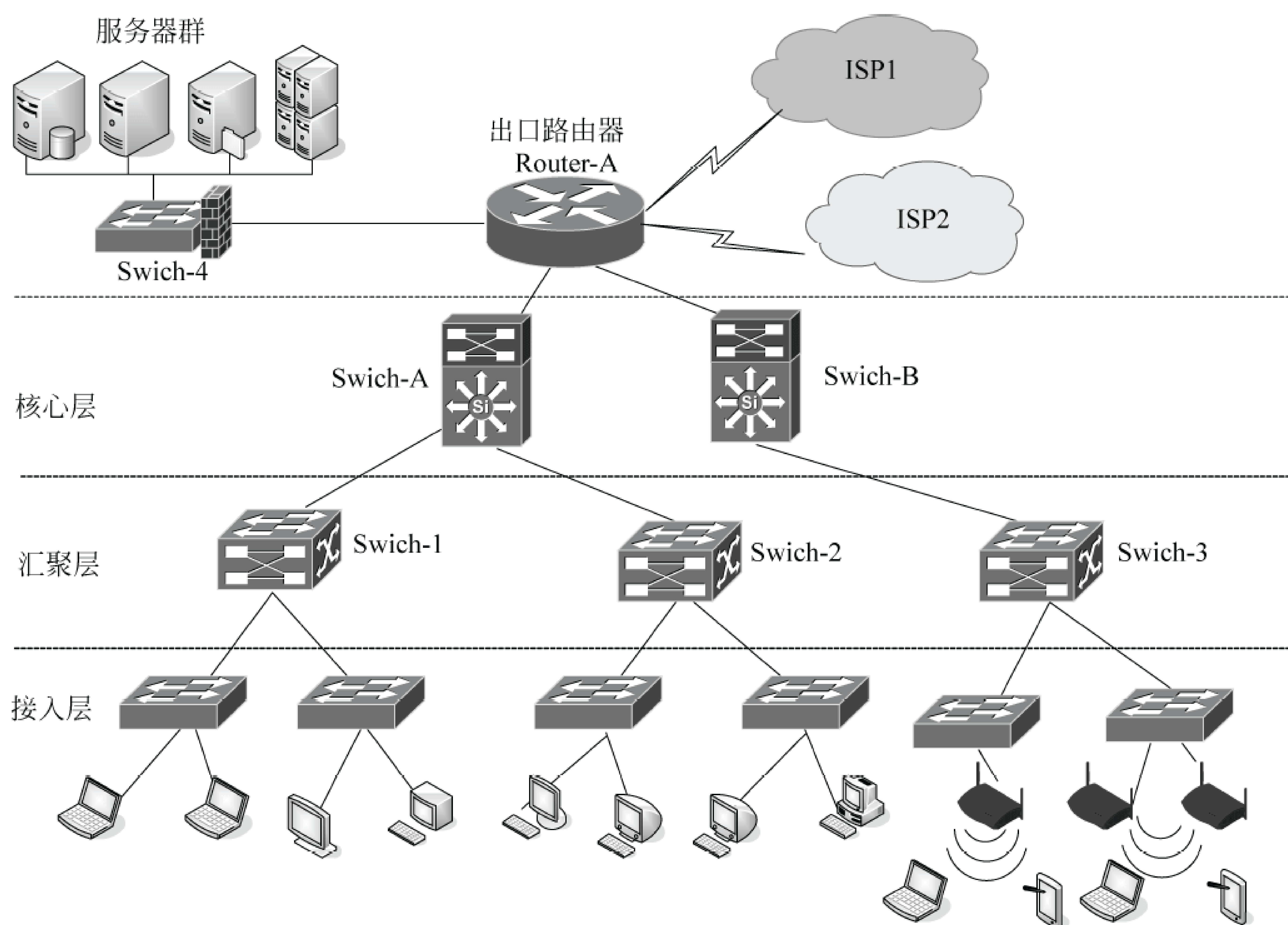


图 1-1

【问题 1】（5 分）

企业网络的可用性和可靠性是至关重要的，经常会出现因网络设备、链路损坏等导致整个网络瘫痪的现象。为了解决这个问题，需要在已有的链路基础上再增加一条备用链路，这称作网络冗余。

（1）对于企业来说，直接增加主干网络链路带宽的方法有哪些？并请分析各种方法的优缺点。（3 分）

（2）一般常用的网络冗余技术可以分为哪两种。（2 分）

【问题 2】（10 分）

（1）网络冗余是当前网络为了提高可用性、稳定性必不可少的技术，在本企业网络中要求使用双核心交换机互做备份实现两种网络冗余技术，同时出口路由器因为负载过重也需要进行网络结构调整优化，请画图说明在不增加网络设备的情况下完成企业主干网络结构调优。（4 分）

（2）在两台核心交换机上配置 VRRP 冗余，以下为部分配置命令。根据需求，完成（或解释）核心交换机 Switch-A 的部分配置命令。（6 分）

```
Switch-A:
Switch-A(config)#track 100 interface F0/1 line-protocol
//_______①_______
Switch-A(config-track)#exit
Switch-A(config)#int VLAN 1
Switch-A(config-if)#vrrp 1 ip 192.168.1.254
//在 VLAN1 中配置 VRRP 组 1，并指定虚拟路由器的 IP 地址为 192.168.1.254
Switch-A(config-if)#_______②_______
//开启主路由器身份抢占功能
Switch-A(config-if)#vrrp 1authentication md5 key-string Cisco
//配置 VRRP 协议加密认证
Switch-A(config-if)#vrrp 1 track 100 decrement 30
//_______________③_______________
```

【问题 3】（6 分）

随着企业网络的广泛应用，用户对于移动接入企业网的需求不断增加，无线网络作为有线网络的有效补充，凭借着投资少、建设周期短、使用方便灵活等特点越来越受到企业的重视，近年来企业也逐步加大无线网络的建设力度。

（1）构建企业无线网络如何保证有效覆盖区域并尽可能减少死角？（2 分）

（2）IEEE 认定的四种无线协议标准是什么？（2 分）

（3）简单介绍三种无线安全的加密方式。（2 分）

【问题 4】（4 分）

随着企业关键网络应用业务的发展，在企业网络中负载均衡的应用需求也越来越大。

（1）负载均衡技术是什么？负载均衡会根据网络的不同层次（网络七层）来划分。其中，第二层的负载均衡是什么技术？（2 分）

（2）服务器集群技术和服务器负载均衡技术的区别是什么？（2 分）

试题一分析

本题主要考查企业网络规划中网络的可靠性。

【问题 1】

本问题主要考查网络冗余技术。

互联网发展速度迅猛，企业对于网络的性能、网速和带宽的要求日益增加，在这种发展势头下，企业网络难免会出现链路带宽不足的现象。对于企业来说，解决链路带宽不足可以采用多种方法来解决。一是直接升级主干网络带宽，如将百兆网络升级为千兆网络，千兆网络升级为万兆网络等，这种升级效果比较明显，但是在升级中不单是要考虑更换网络连接线缆，很多设备往往也要更换，因此需要结合企业的经济状况和业务需求综合考虑。

另外一种方法是将关键设备间的链路数量增加，这样一来升级成本就大大降低。但是直接在设备之间连接多条线缆的话可能会造成环路，导致广播风暴。所以还要采用相应的技术限制环路的产生，一般这里使用的技术被称为以太网信道或者端口聚合。使用该技术首先需要两端的设备都要支持端口聚合技术（以太网信道技术），同时进行端口捆绑的多个接口状态必须相同，如带宽、速度、双工模式等，最好用相邻的端口。

随着 Internet 的发展，大型园区网络从简单的信息承载平台转变成一个公共服务提供平台。作为终端用户，希望能时时刻刻保持与网络的联系，因此健壮、高效和可靠成为园区网发展的重要目标，而要保证网络的可靠性，就需要使用到冗余技术。高冗余网络就是在网络设备、链路发生中断或者变化的时候，用户几乎感觉不到。一般常用的网络冗余技术可以分作二层链路冗余和三层网关冗余。在二层链路中实现冗余的方式主要有两种，生成树协议和链路捆绑技术。其中生成树协议是一个纯二层协议，但是链路捆绑技术在二层接口和三层接口上都可以使用。三层链路冗余技术较二层链路冗余技术丰富很多，依靠各种路由协议可以实现三层链路冗余和负载均衡。另外三层链路捆绑技术也提供了路由协议之外的一种选择。对于使用网络的终端用户来讲，也需要一种机制来保证其与园区网络的可靠连接，这就是三层网关级冗余技术。VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）、HSRP（Hot Stand by Router Protocol，热备份路由器协议）及 GLBP（Gateway Load Balancing Protocol，网关负载均衡协议）都是比较常用的网关冗余方法。但是 HSRP 和 GLBP 是思科的专有协议，VRRP 协议是开放的。所以在设备比较复杂的大型网络里面，大都使用 VRRP 协议实现网关冗余。

【问题 2】

本问题主要考查网络的优化及基于 VLAN 的多层网络冗余配置。

在图 1-1 中，整个企业网络在网络冗余方面几乎没有做任何设置，如两台核心交换机之间没有互联，汇聚交换机到核心交换机之间没有链路冗余，这样主干网的带宽和链路冗余都得不到保障，因此整个网络的可靠性会很差。其次，在网络出口路由器上接入了服务器群，这样在网络进出口流量比较大的时候，出口路由器负担就会比较重，会影响网络的正常访问速度，需要调整服务器群的接入位置。

如图 1-2 所示，优化整个网络布局。其中虚线为增加的链路。首先在两台核心交换

机之间实现链路聚合以增加主干网络带宽。其次按照图中的连接方法已经构成了二层环路，链路冗余已经产生，关键是要把两台核心交换机定义为 STP 的根桥；三层网关冗余技术主要是做网关备份，因此，需要在双核心交换机上配置 VRRP 协议。最后为了减少出口路由器的负担，考虑把服务器群接入到核心交换机 A 或者 B 上。

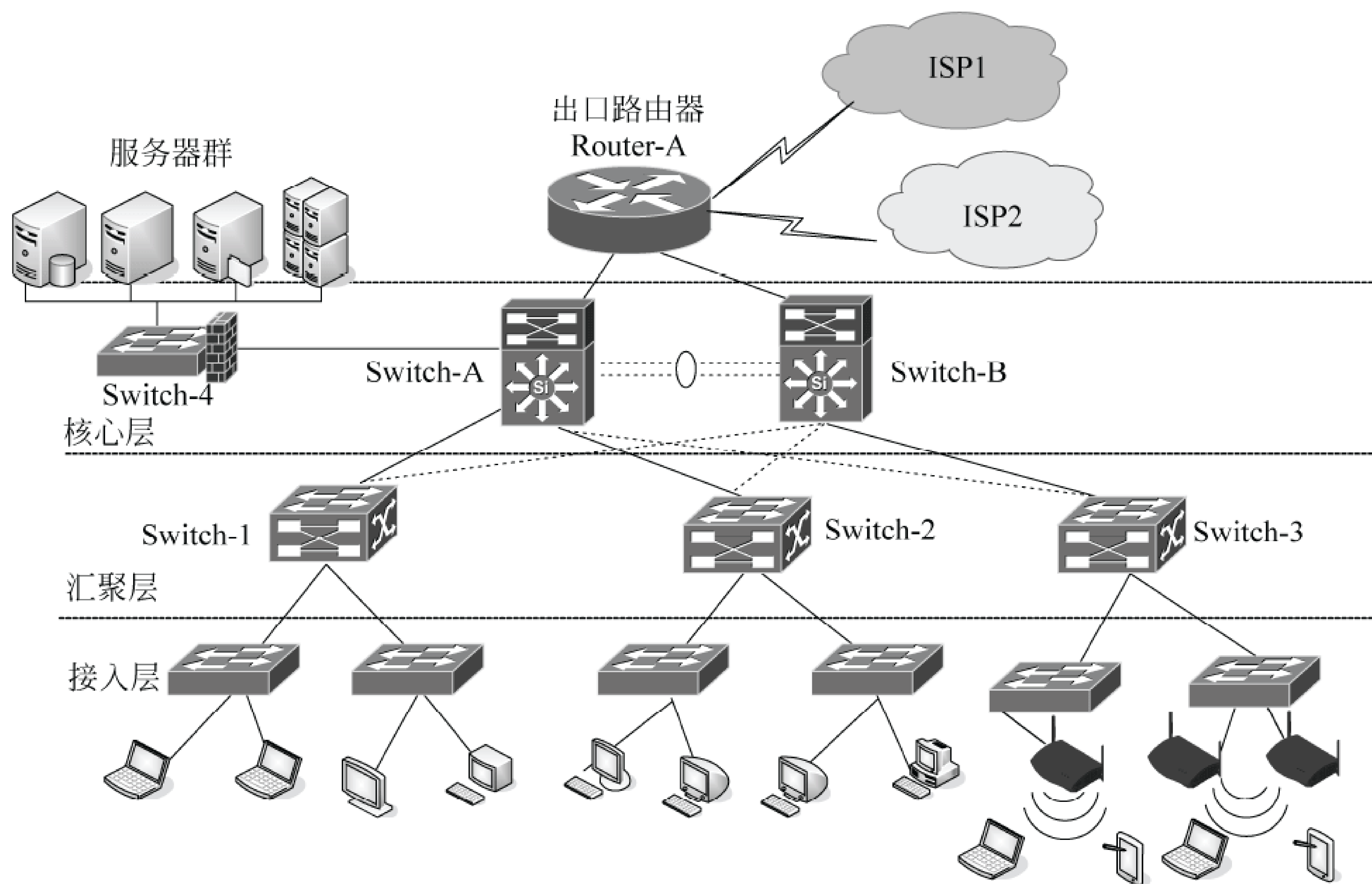


图 1-2 优化后的企业网络拓扑图

三层链路冗余技术主要是做网关备份，在配置之前首先要确保网络访问畅通。所以要正确配置接口 IP 地址及合适的路由。在配置网关冗余时主要使用 VRRP 协议，每一个 VLAN 作为一个 VRRP 组进行配置，按照题目要求，为双核心三层交换机的 VLAN 配置 VRRP 协议的部分配置命令如下：

```
Switch-A:
Switch-A(config)#track 100 interface F0/1 line-protocol
//开启路由器端口跟踪功能，当三层交换机上端链路故障时可通过接口 F0/1 的跟踪功能判断整
  条链路故障，从而使 VRRP 主路由器身份跳转
Switch-A(config-track)#exit
Switch-A(config)#int VLAN 1
Switch-A(config-if)#vrrp 1 ip 192.168.1.254
//在 VLAN1 中配置 VRRP 组 1，并指定虚拟路由器的 IP 地址为 192.168.1.254
Switch-A(config-if)# vrrp 1 preempt
//开启主路由器身份抢占功能
Switch-A(config-if)#vrrp 1authentication md5 key-string Cisco
```

```
//配置 VRRP 协议加密认证
Switch-A(config-if)#vrrp 1 track 100 decrement 30
//端口跟踪，当发现链路故障时，自动将优先级降低 30，以便其他可用链路的设备抢夺 VRRP
  主路由器身份
```

【问题 3】

本问题主要考查 WLAN 无线网络建设的相关知识。

（1）在架设无线网络过程中，因为无线网络并不像有线网络那么直观，所以在架设无线网络时一般为了减少死角，必须让两个相邻的 AP 覆盖的无线区域重叠。因为一个 AP 覆盖的无线网络区域一般是球形的，只有两个区域部分相互重叠才能确保无线信号更全面。除此之外，选择 AP 时也要考虑当前物理环境，如果是空旷的环境可以选择使用放射信号为球形的 AP 设备（全向天线），如果是在楼层中可以考虑使用向某个区域放射信号的 AP 设备（定向天线）。

（2）目前，主流的无线协议都是由 IEEE 所制定，IEEE 认定的四种无线协议标准分别为 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 和 IEEE 802.11n。IEEE 802.11a 标准工作在 5GHzU-NII 频带，物理层速率最高可达 54Mbps，传输层速率最高可达 25Mbps。IEEE 802.11b 是无线局域网的一个标准。其载波的频率为 2.4GHz，传送速度为 11Mbit/s。IEEE 802.11b 是所有无线局域网标准中最著名，也是普及最广的标准。IEEE 802.11b 的后继标准是 IEEE 802.11g，其载波的频率为 2.4GHz（跟 802.11b 相同），原始传送速度为 54Mbit/s，净传输速度约为 24.7Mbit/s（跟 802.11a 相同）。IEEE 802.11n 于 2009 年 9 月正式批准。使用 2.4GHz 频段和 5GHz 频段，传输速度 300Mbps，最高可达 600Mbps，可向下兼容 802.11b、802.11g。

（3）无线网络通过无线信号进行信息传输，数据的安全性难以保障，因此为了保障无线网络数据的安全性，各种各样的无线加密算法应运而生。第一种：WEP 加密，WEP（有线对等保密）协议，它主要用于 WLAN 中链路层信息数据的加密，采用的是静态的密钥。第二种：WPA 加密，如 WPA 和 WPA2，WPA 算法主要用于增强 WLAN 系统的数据保护和访问控制水平，采用了动态的密钥，WPA2 是在 WPA 的基础之上经 WiFi 联盟验证过的 IEEE 802.11i 标准的验证形式，是目前公认的比较安全的无线加密算法。第三种：WPA-PSK 加密，如 WPA-PSK 和 WPA2-PSK，由于 WPA 操作复杂，因此经常采用其简化版 WPA-PSK 和 WPA2-PSK，不需要设置复杂的身份证明等信息，因而在实际使用中最为普遍。

【问题 4】

本问题主要考查负载均衡技术的相关知识。

（1）负载均衡（Load Balancing）技术建立在现有网络结构之上，它提供了一种廉价有效透明的方法，扩展网络设备和服务器的带宽，增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。

负载均衡有两方面的含义：首先，单个重负载的运算分担到多台节点设备上做并行处理，每个节点设备处理结束后，将结果汇总，返回给用户，系统处理能力得到大幅度提高，这就是常说的集群（Clustering）技术。第二层含义就是：大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间，这主要针对 Web 服务器、FTP 服务器、企业关键应用服务器等网络应用。通常，负载均衡会根据网络的不同层次（网络七层）来划分。其中，第二层的负载均衡指将多条物理链路当作一条单一的聚合逻辑链路使用，这就是链路聚合（Trunking）技术，它不是一种独立的设备，而是交换机等网络设备的常用技术。现代负载均衡技术通常操作于网络的第四层或第七层，这是针对网络应用的负载均衡技术，它完全脱离于交换机、服务器而成为独立的技术设备。近年来，四到七层网络负载均衡首先在电信、移动、银行、大型网站等单位进行了应用，因为其网络流量瓶颈的现象最突出。这也就是为何每通一次电话，就会经过负载均衡设备的原因。另外，在很多企业，随着企业关键网络应用业务的发展，负载均衡的应用需求也越来越大了。

（2）集群（Cluster）：集群就是一组连在一起的计算机，从外部看它是一个系统，各节点可以是不同的操作系统或不同硬件构成的计算机。如一个提供 Web 服务的集群，对外界来看是一个大 Web 服务器。不过集群的节点也可以单独提供服务。因此可以说集群是一组独立的计算机系统构成一个松耦合的多处理器系统，它们之间通过网络实现进程间的通信。应用程序可以通过网络共享内存进行消息传送，实现分布式计算机。主要解决高可靠性（HA）和高性能计算（HP）。

负载均衡建立在现有网络结构之上，它提供了一种廉价有效的方法扩展服务器带宽和增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。它主要完成以下任务：解决网络拥塞问题，服务就近提供，实现地理位置无关性；为用户提供更好的访问质量；提高服务器响应速度；提高服务器及其他资源的利用效率；避免了网络关键部位出现单点失效。

区别是集群系统（Cluster）主要解决下面几个问题：高可靠性（HA），利用集群管理软件，当主服务器故障时，备份服务器能够自动接管主服务器的工作，并及时切换过去，以实现对用户的不间断服务；高性能计算（HP）：即充分利用集群中的每一台计算机的资源，实现复杂运算的并行处理，通常用于科学计算领域，比如基因分析，化学分析等。负载平衡：即把负载压力根据某种算法合理分配到集群中的每一台计算机上，以减轻主服务器的压力，降低对主服务器的硬件和软件要求。主要解决的是大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间。

参考答案

【问题 1】

（1）一般有两种方法，一是直接升级主干网络带宽。优点是效果显著，不足之处是这种方法投入较大；二是采用以太网信道或者端口聚合技术。优点是投入较小，缺点是

使用该技术需要两端设备都支持端口聚合技术，且进行端口捆绑的多个接口状态必须相同。

（2）一般常用的网络冗余技术可以分为二层链路冗余和三层网关冗余。

【问题 2】

（1）如图 1-3 所示，虚线为增加的链路。首先在两台核心交换机之间实现链路聚合以增加主干网络带宽。其次是要把两台核心交换机定义为 STP 的根桥；同时要做网关备份，主要是在双核心交换机上配置 VRRP 协议。最后为了减少出口路由器的负担，考虑把服务器群接入到核心交换机 A 或者 B 上。

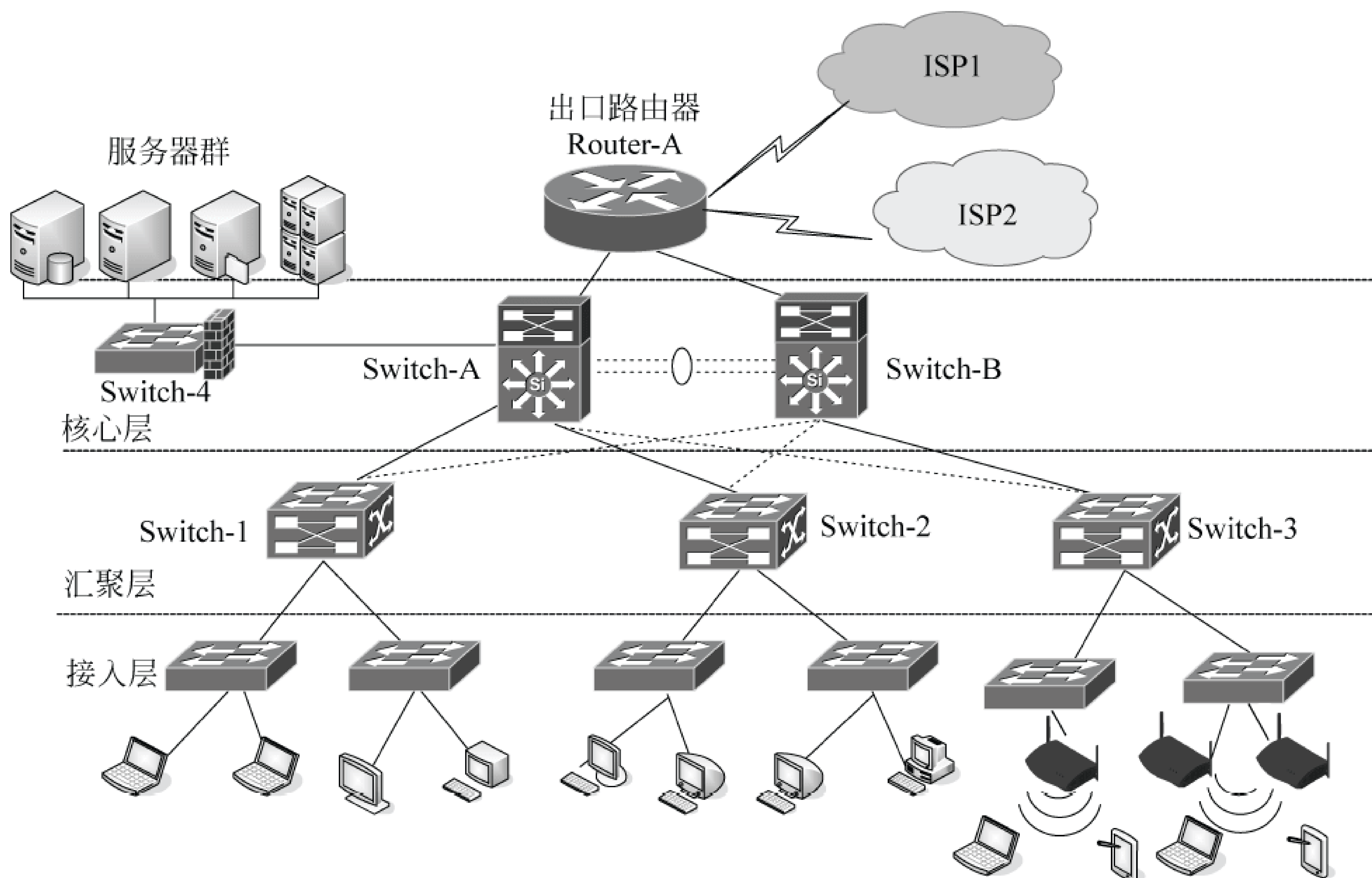


图 1-3　优化后的企业网络拓扑图

（2）① 开启路由器端口跟踪功能。

② vrrp 1 preempt。

③ 端口跟踪，当发现链路故障时，自动将优先级降低 30，以便其他可用链路的设备抢夺 VRRP 主路由器身份。

【问题 3】

（1）构建企业无线网络为了减少死角，必须让两个 AP 覆盖的无线区域重叠。除此之外，选择 AP 时也要考虑当前物理环境，如果是空旷的环境可以选择使用放射信号为球形的 AP 设备，如果是在楼层中可以考虑使用向某个区域放射信号的 AP 设备。

（2）目前，主流的无线协议都是由 IEEE 所制定，IEEE 认定的四种无线协议标准分别为 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 和 IEEE 802.11n。

（3）第一种：WEP 加密 WEP（有线对等保密）协议

第二种：WPA 加密 WPA 和 WPA2

第三种：WPA-PSK 加密 WPA-PSK 和 WPA2-PSK

【问题 4】

（1）负载均衡（Load Balancing）技术建立在现有网络结构之上，它提供了一种廉价有效透明的方法，扩展网络设备和服务器的带宽，增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。

第二层的负载均衡指将多条物理链路当作一条单一的聚合逻辑链路使用，即链路聚合（Trunking）技术。

（2）集群（Cluster）：是一组独立的计算机系统构成一个松耦合的多处理器系统，它们之间通过网络实现进程间的通信。应用程序可以通过网络共享内存进行消息传送，实现分布式计算。主要解决高可靠性（HA）和高性能计算（HP）。

负载均衡技术提供了一种廉价有效的方法，扩展服务器带宽和增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。主要解决的是大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间。

试题二（共 25 分）

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

某高校校园网使用 3 个出口，新老校区用户均通过老校区出口访问互联网，其中新老校区距离 20 公里，拓扑结构如图 2-1 所示，学校服务器区网络拓扑结构如图 2-2 所示。

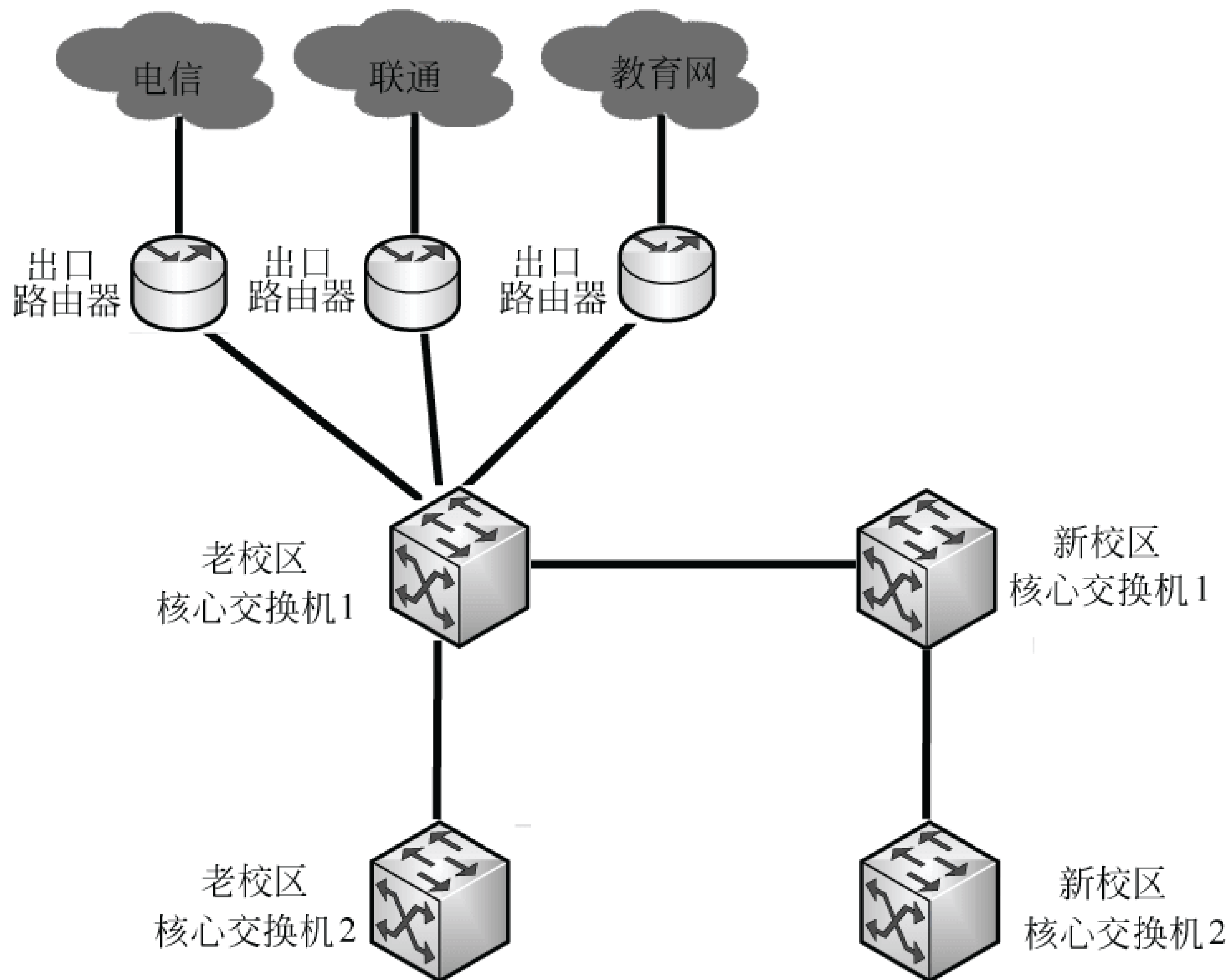


图 2-1 拓扑结构图 1

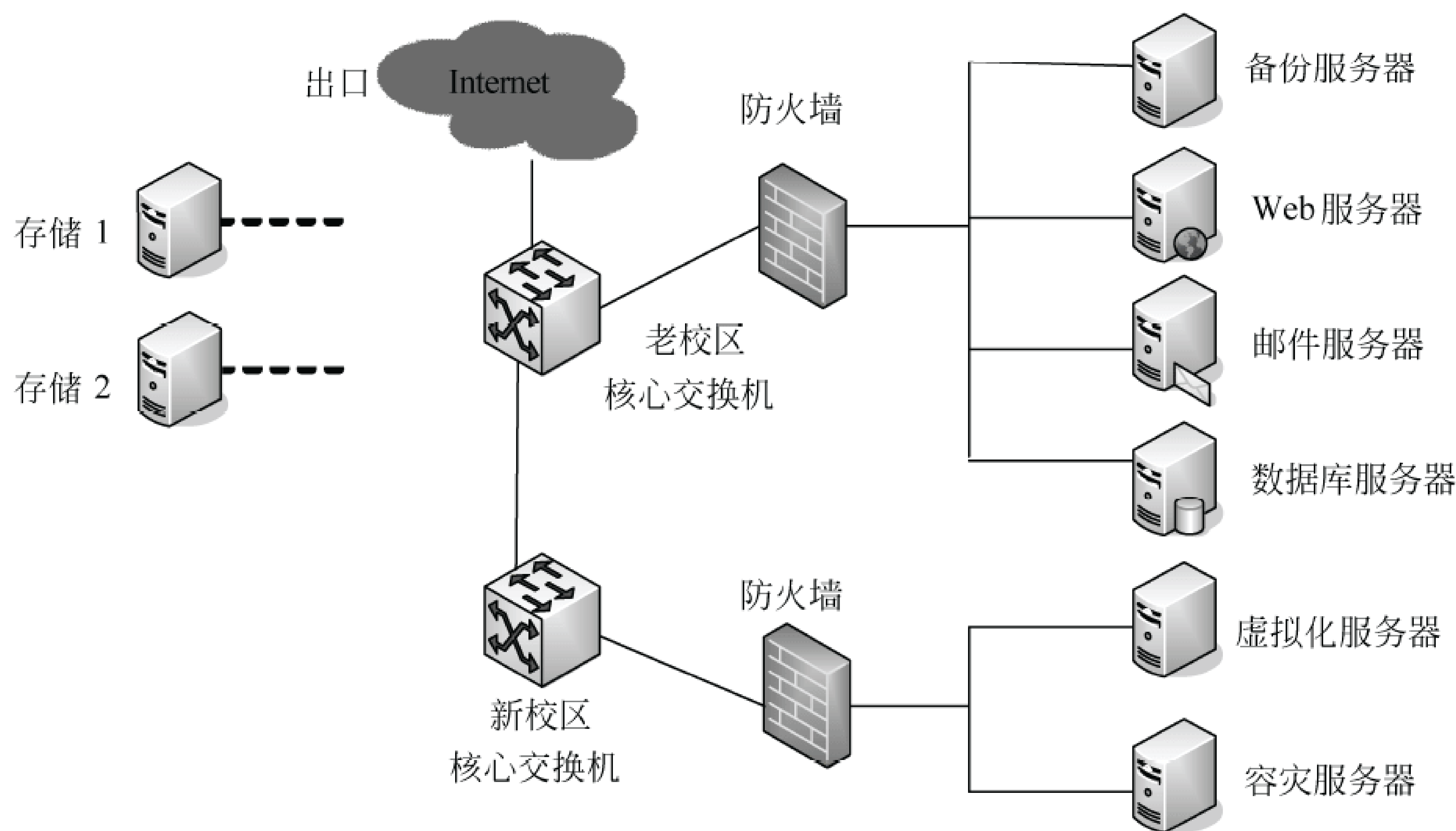


图 2-2 拓扑结构图 2

【问题 1】（3 分）

实现多出口负载均衡通常有依据源地址和目标地址两种方式，分别说明两种方式的实现原理和特点。

【问题 2】（7 分）

根据学校多年实际运行情况，现需对图 2-1 所示网络进行优化改造，要求：

（1）在只增加负载均衡设备的情况下，且仅限通过老校区核心交换机 1 连接出口路由器；

（2）采用网络的冗余，解决新老校区互联网络中的单点故障；

（3）通过多出口线路负载，解决单链路过载；

（4）考虑教育网的特定应用，需采用明确路由。

试画出图 2-1 优化后的网络拓扑结构，并说明改造理由。

【问题 3】（5 分）

现学校有两套存储设备，均放置于老校区中心机房，存储 1 是基于 IP-SAN 技术，存储 2 是基于 FC-SAN 技术。试说明图 2-2 中数据库服务器和容灾服务器应采用哪种存储技术，并说明理由。

【问题 4】（5 分）

当前存储磁盘柜中通常包含 SAS 和 SATA 磁盘类型，试说明图 2-2 中数据库服务器和容灾服务器各应选择哪种磁盘类型，并说明理由。

【问题 5】（5 分）

目前存储中使用较多的是 RAID5 和 RAID10，试说明图 2-2 中数据库服务器和容灾服务器（数据级）各应选择哪种 RAID 技术，并说明理由。

试题二分析

本题考查网络规划和优化的相关知识，涉及网络负载均衡、网络存储系统。

【问题 1】

本问题考查依据源地址和目的地址的负载均衡的实现原理和优缺点，是理论性知识。依据源地址负载均衡根据源 IP 地址来选择不同外网出口，可以根据各出口带宽按比例划分对应的源 IP 子网段，达到出口负载均衡的作用，但是访问同一资源时，部分用户响应快，部分用户响应慢。

依据目的地址负载均衡根据目的 IP 地址来选择不同外网出口，内部用户可以根据不同运营商提供的资源，选择相应运营商的出口，但是会导致提供资源丰富的运营商出口负载过大，提供资源相对比较少的运营商出口负载很轻，造成各出口不均衡的现象。

【问题 2】

整合改造方案中，要根据题目中的限制条件进行设计优化改造方案。

根据题目要求，可以看出需要改造的地方：

（1）将 4 台核心交换机组成环网结构，避免新老校区设备或单链路故障造成新老校区网络中断；

（2）在电信、联通链路增加负载均衡设备，平衡各出口的负载和加快内部用户访问外网的速度；

（3）同时考虑教育网的特定应用，配置教育网走明确路由。

【问题 3】

本问题考查 IP-SAN 技术和 FC-SAN 技术的优缺点，结合实际应用选择。

（1）容灾服务器：容灾服务器和存储设备距离 20 公里，需要远距离传输，所以只能选择 IP-SAN 技术。

（2）数据库服务器：需要高性能、大并发、快速响应，最合理应该选择 FC-SAN 技术。

【问题 4】

数据库服务器和容灾服务器相比，数据库服务器数据容量小，读写频繁，要求速度快，而容灾服务器不追求速度，侧重于大容量。

所以综合 SAS 磁盘和 SATA 磁盘在传输速率、安全型和性价比方面的优缺点，采取数据库服务器选择 SAS 磁盘，容灾服务器选择 SATA 磁盘。

【问题 5】

数据库服务器性能、安全级别都比容灾服务器要求高，所以数据库服务器选择 RAID10，容灾服务器选择 RAID5。原因如下：

（1）I/O：读操作上，RAID10 和 RAID5 是相当的，写操作上，RAID10 好于 RAID5；
（2）数据重构：在一块磁盘失效，进行数据重构期间，RAID5 要比 RAID10 耗时长，负荷大，数据丢失可能性高，可靠性低。

参考答案

【问题 1】

依据源地址负载均衡：根据源 IP 地址来选择不同外网出口，可以根据各出口带宽按比例划分对应的源 IP 子网段，达到出口负载均衡的作用，但是访问同一资源时，部分用户响应快，部分用户响应慢。

依据目的地址负载均衡：根据目的 IP 地址来选择不同外网出口，内部用户可以根据不同运营商提供的资源，选择相应运营商的出口，但是会导致提供资源丰富的运营商出口负载过大，提供资源相对比较少的运营商出口负载很轻，造成各出口不均衡的现象。

【问题 2】

改造后的出口网络拓扑如图 2-3 所示。

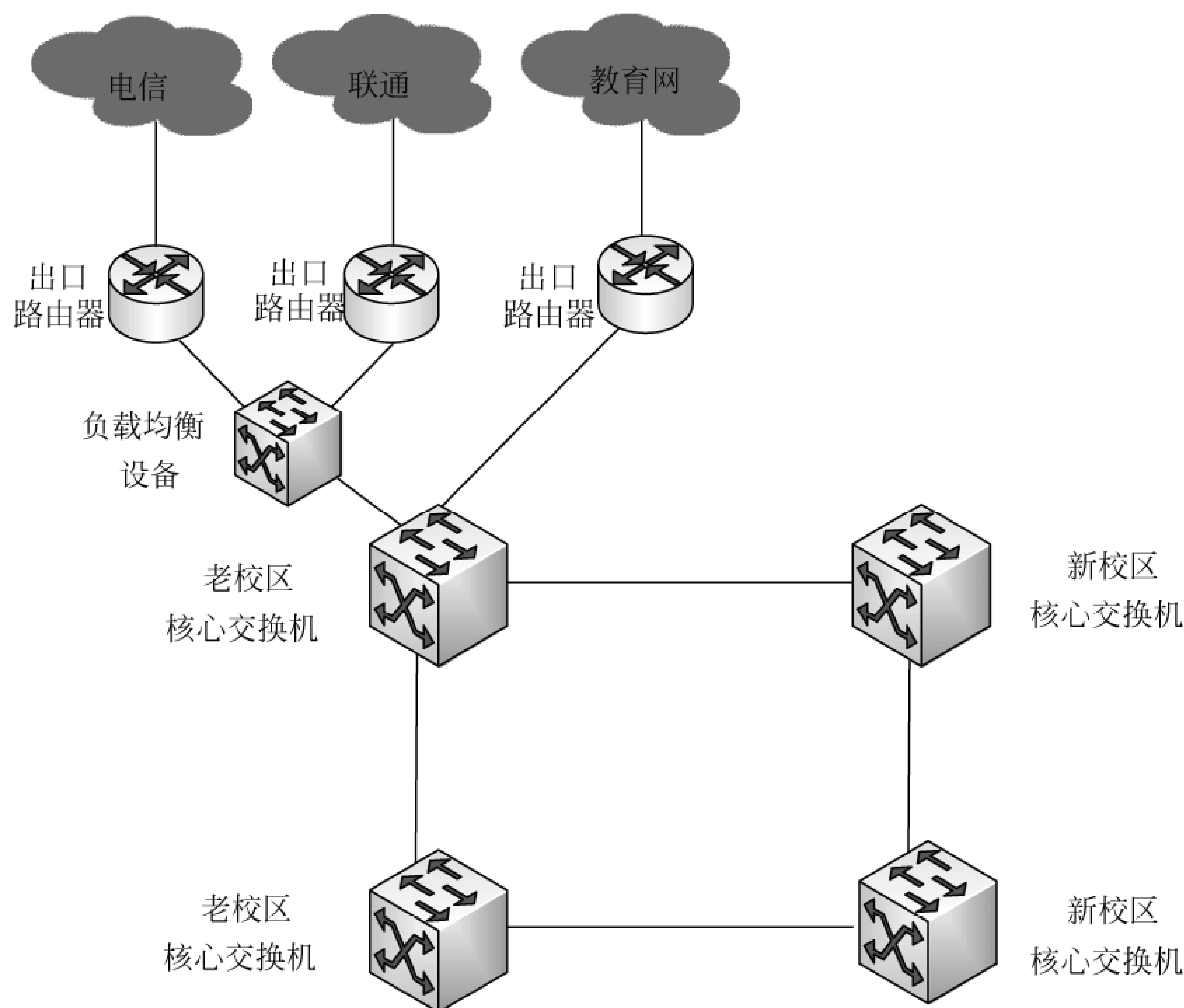


图 2-3　改造后的出口网络拓扑

改造原因：

（1）将 4 台核心交换机组成环网结构，避免新老校区设备或单链路故障造成新老校区网络中断；

（2）在电信、联通链路增加负载均衡设备，平衡各出口的负载和加快内部用户访问外网的速度；

（3）同时考虑教育网的特定应用，配置教育网走明确路由。

【问题 3】

（1）容灾服务器：容灾服务器和存储设备距离 20 公里，需要远距离传输，所以只能选择 IP-SAN 技术；

（2）数据库服务器：需要高性能、大并发、快速响应，最合理的应该选择 FC-SAN 技术。

【问题 4】

数据库服务器选择 SAS 磁盘，容灾服务器选择 SATA 磁盘。原因如下：

（1）SAS 是双端口，采用全双工的工作方式传输数据，而 SATA 是单端口，采用半双工的工作方式传输数据；

（2）SAS 使用 SCSI 命令进行错误校正和错误报告，这比 SATA 采用的 ATA 命令集有更多的功能；

（3）SAS 磁盘容量小， 价格比较昂贵，SATA 磁盘容量大，价格比较便宜。

【问题 5】

数据库服务器选择 RAID10，容灾服务器选择 RAID5。原因如下：

（1）I/O：读操作上，RAID10 和 RAID5 是相当的，写操作上，RAID10 好于 RAID5；

（2）数据重构：在一块磁盘失效，进行数据重构期间，RAID5 要比 RAID10 耗时长，负荷大，数据丢失可能性高，可靠性低。

试题三（共 25 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

某高校网络拓扑结构如图 3-1 所示。

【问题 1】（7 分）

目前网络中存在多种安全攻击，需要在不同的位置部署不同的安全措施进行防范。常见的安全防范措施有：

1. 防非法 DHCP 欺骗
2. 用户访问权限控制技术
3. 开启环路检测（STP）
4. 防止 ARP 网关欺骗
5. 广播风暴的控制
6. 并发连接数控制
7. 病毒防治

其中：在安全设备 1 上部署的措施有：____（1）____；

在安全设备 2 上部署的措施有：____（2）____；

在安全设备 3 上部署的措施有：____（3）____；

在安全设备 4 上部署的措施有：____（4）____。

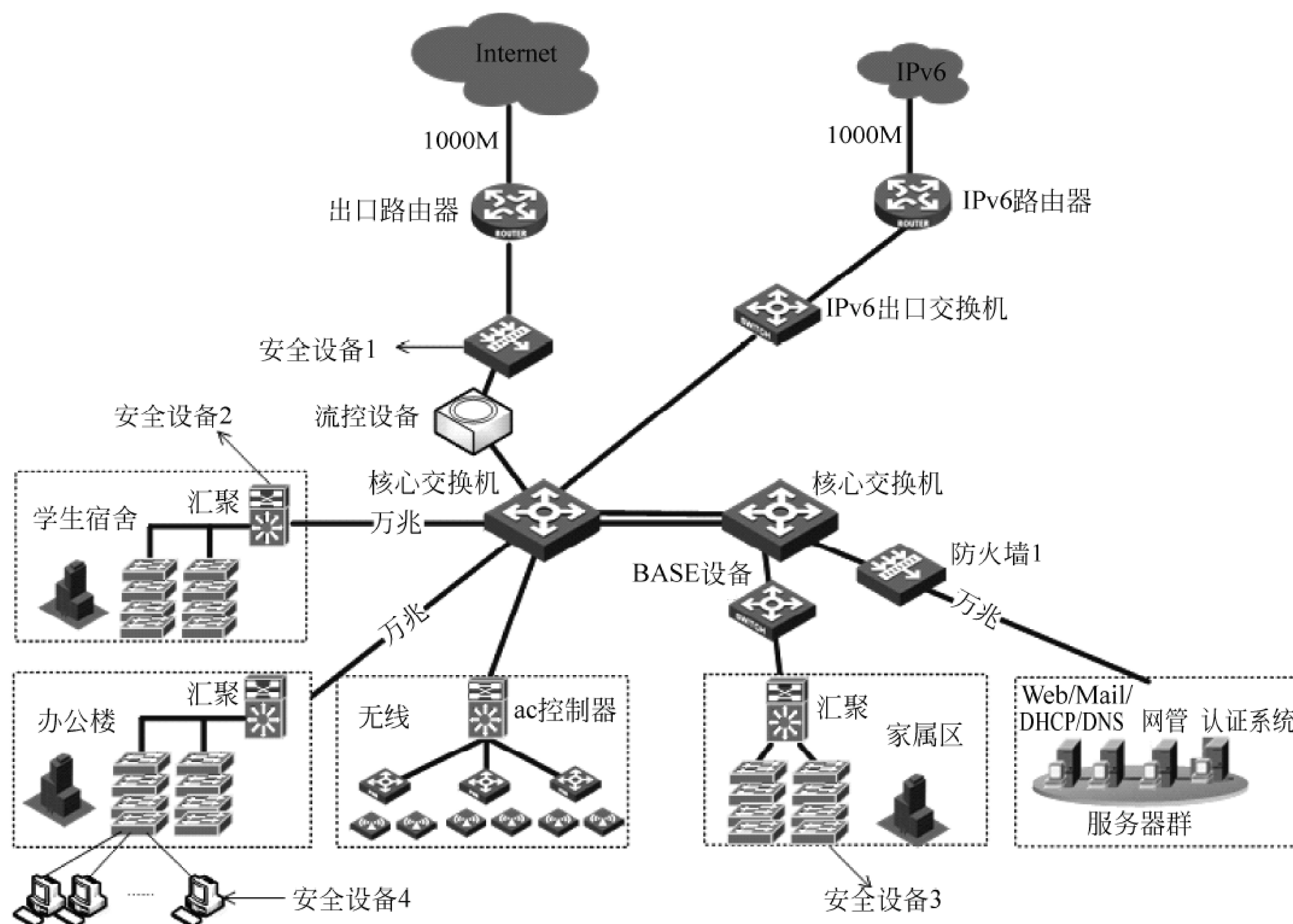


图 3-1　某高校网络拓扑结构图

【问题 2】（8 分）

学校服务器群目前共有 200 台服务器为全校提供服务，为了保证各服务器能提供正常的服务，需对图 3-1 所示防火墙 1 进行安全配置，设计师制定了 2 套安全方案，请根据实际情况选择合理的方案并说明理由。

方案一：根据各业务系统的重要程度，划分多个不同优先级的安全域，每个安全域采用一个独立子网，安全域等级高的主机默认允许访问安全域等级低的主机，安全域等级低的主机不能直接访问安全域等级高的主机，然后根据需要添加相应安全策略。

方案二：根据各业务系统提供的服务类型，划分为数据库、Web、认证等多个不同虚拟防火墙，同一虚拟防火墙中相同 VLAN 下的主机可以互访，不同 VLAN 下的主机均不允许互访，不同虚拟防火墙之间主机均不能互访。

【问题 3】（6 分）

为了防止资源的不合理使用，通常在核心层架设流控设备进行流量管理和终端控制，请列举出 3 种以上流控的具体实现方案。

【问题 4】（4 分）

非法 DHCP 欺骗是网络中常见的攻击行为，说明其实现原理并说明如何防范。

试题三分析

本题主要考查园区网络安全设计。

【问题 1】

本问题主要考查安全技术加载的位置。

从 DHCP 工作原理可以看出，如果客户端是第一次、重新登录或租期已满不能更新租约，客户端都是以广播的方式来寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，如果在网络中存在多台 DHCP 服务器（有一台或更多台是非授权的），谁先应答，客户端就采用其提供的网络配置参数。假如非授权的 DHCP 服务器先应答，这样客户端最后获得的网络参数即是非授权的，客户端即被欺骗了。而在实际应用 DHCP 的网络中，基本上都会采用 DHCP 中继，这样的话，本网络的非授权 DHCP 服务器一般都会先于其余网络的授权 DHCP 服务器的应答（由于网络传输的延迟），在这样的应用中，DHCP 欺骗更容易完成。对 DHCP 欺骗的防范方法主要是在交换机上启用 DHCP SNOOPING 功能。

用户访问权限控制通常读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。通常加载在汇聚层交换机上。

频繁改动网络时很容易引发网络环路，网络环路引起的网络堵塞现象常常具有较强的隐蔽性，不利于故障现象的高效排除。开启环路检测（STP）通常加载在接入交换机上，通过配置交换机的环回监测功能，快速地判断局域网中是否存在网络环路。

ARP 网关欺骗是局域网中一台机器，反复向其他机器，特别是向网关，发送假冒的 ARP 应答信息包，造成严重的网络堵塞。解决的方法是在某个网络内采用检测技术，防止欺骗。

并发连接数控制整个网络中的连接数，需在核心层完成。

病毒防治在网络内，通常在单机上完成。

【问题 2】

本问题主要考查防火墙安全技术的设计。

方案一按照主机添加安全策略，防火墙的安全策略数量比较多，对防火墙的资源消耗也会比较大，方案二按照服务添加安全策略，所以防火墙安全策略数量不多，对防火墙的资源消耗也会比较小。

如果某一主机感染病毒或木马时，方案一安全域级别低或者相同的其他主机会受到影响，方案二相同虚拟防火墙中相同 VLAN 主机会受到影响，其余主机不会影响；而且后期服务器数量大幅增加，方案一需新增加多条安全策略，方案二服务类型不新增的情况下，安全策略基本不需增加。

综上，选择方案二。

【问题 3】

本问题主要考查流量管理的实现技术。

通常在核心层架设流控设备进行流量管理和终端控制，有以下 3 种：

（1）针对地址进行带宽限制。针对源 IP 地址、目的 IP 地址进行带宽限制，防止某地址独占带宽。

（2）针对子网进行带宽限制。针对子网进行带宽限制，防止某子网独占带宽，如某个部门划分一个子网。

（3）针对服务进行带宽限制。针对服务进行带宽限制，防止某服务独占带宽，如视频、BT 等。

【问题 4】

本问题主要考查非法 DHCP 欺骗原理。

客户端第一次登录、重新登录或租期已满不能更新租约时，以广播方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，如果在网络中存在多台 DHCP 服务器（有一台或更多台是非授权的），并且非授权的 DHCP 服务器先应答，那么客户端就会获得非授权的网络参数。可以在交换机上开启 DHCP SNOOPING，通过建立和维护 DHCP SNOOPING 绑定表并过滤不可信任的 DHCP 信息，只让合法的 DHCP 应答通过交换机，阻断非法应答，从而防止 DHCP 欺骗。

参考答案

【问题 1】

（1）6. 并发连接数控制

（2）2. 用户访问权限控制技术

（3）1. 防非法 DHCP 欺骗

3. 开启环路检测（STP）

4. 防止 ARP 网关欺骗

5. 广播风暴的控制

（4）7. 病毒防治

【问题 2】

1. 选择方案二

2. 理由：

（1）如果服务器规模比较大，方案一按照主机添加安全策略，所以防火墙的安全策略数量比较多，对防火墙的资源消耗也会比较大，方案二按照服务添加安全策略，所以防火墙安全策略数量不多，对防火墙的资源消耗也会比较小；

（2）如果某一主机感染病毒或木马时，方案一安全域级别低或者相同的其他主机会受到影响，方案二相同虚拟防火墙中相同 VLAN 主机会受到影响，其余主机不会影响；

（3）后期服务器数量大幅增加，方案一需新增加多条安全策略，方案二服务类型不

新增的情况下，安全策略基本不需增加。

【问题 3】

（1）针对地址进行带宽限制。针对源 IP 地址、目的 IP 地址进行带宽限制，防止某地址独占带宽。

（2）针对子网进行带宽限制。针对子网进行带宽限制，防止某子网独占带宽，如某个部门划分一个子网。

（3）针对服务进行带宽限制。针对服务进行带宽限制，防止某服务独占带宽，如视频、BT 等。

【问题 4】

1．非法 DHCP 欺骗原理：客户端第一次登录、重新登录或租期已满不能更新租约时，以广播方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，如果在网络中存在多台 DHCP 服务器（有一台或更多台是非授权的），并且非授权的 DHCP 服务器先应答，那么客户端就会获得非授权的网络参数。

2．防范：可以在交换机上开启 DHCP SNOOPING，通过建立和维护 DHCP SNOOPING 绑定表并过滤不可信任的 DHCP 信息，只让合法的 DHCP 应答通过交换机，阻断非法应答，从而防止 DHCP 欺骗。

第 18 章　2013 下半年网络规划设计师下午试卷 II 写作要点

试题一　论云计算的体系架构和关键技术

云计算是一种网络计算模式，在这种模式下可以随时随地、方便快捷地按需使用互联网上的计算资源。自从 2006 年 Google 等公司提出了云计算的构想以来，这种计算模式得到了学术界和工业界的广泛关注，近年来出现了众多研究成果和云计算平台，许多云计算服务已经出现在各种终端应用上。政府和企业都把云计算作为战略竞争的关键技术，在财力和物力上进行了大量的投入。

请围绕“云计算的体系架构和关键技术”论题，从以下三个方面进行论述。

1．通过应用实例解释云计算的基本概念。

2．就下面的分层模型简要描述云计算的体系架构，各个层次包含的主要构件和需要解决的主要问题。

用户访问接口
管理中间件
资源池
物理资源

3．选择云计算的关键技术进行深入论述，例如数据存储技术、虚拟化技术、任务调度技术、编程模型等（或者你熟悉的其他技术）。

写作要点

1．云计算的基本概念和应用实例

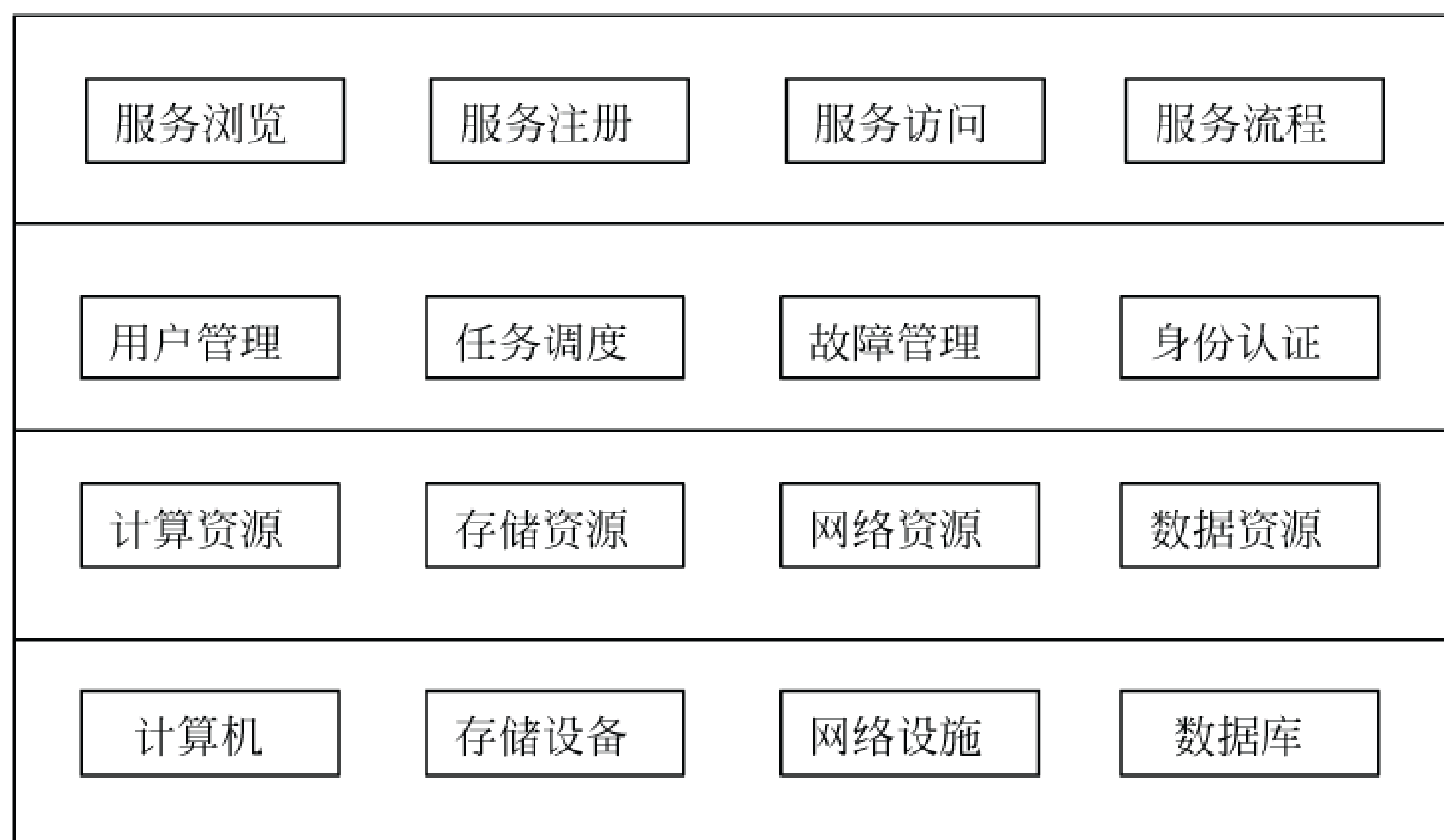
从用户的角度看，云计算是一种信息基础设施，包含硬件设备、软件平台、系统管理和信息服务设施，用户可以按照需求定制云服务，利用网络资源进行需要的计算，而系统维护和安全管理都由云端负责，用户只需按照使用的服务量支付一定的费用。云计算真正实现了用户像使用自来水和电力一样使用网络计算机资源的梦想。

云安全是网络信息安全方面的新进展。通过对网络中大量客户端的监测，可以获得互联网中各种恶意程序发生的最新信息，并推送到服务器端进行分析和处理，再把有关病毒和木马的解决方案分发到各个客户端。云计算强大的数据处理能力和同步调度能力

极大地提升了网络安全公司对新威胁的响应速度。

云计算对信息检索带来了巨大影响。云存储改变了数据存储的模式，由单个服务器独立存储变成了分布式存储基础上的集中数据管理，从而可以使过去在单个服务器上的串行检索改变为云存储模式下的分布式并行数据处理。当云服务界面中的检索代理接受了用户的信息检索请求时，就将检索提问分发给云端的各个存储服务器，分布式检索的结果在检索代理中进行相关度排序后呈现在用户面前。

2．云计算的体系架构



3．云计算的关键技术

数据存储技术：采用分布式文件系统实现海量数据的分布式存储，分布式数据库技术用以实现结构化数据检索服务。

虚拟化技术：实现物理资源的逻辑抽象和统一表示，可以根据用户需求进行资源配置，实现动态的负载均衡，并通过自愈功能来提高系统的可靠性。

任务调度技术：求解的问题被拆分为若干子任务，分派到若干云节点中进行分布式计算，通过多个处理器协同工作，并将计算结果进行排序、合并和汇总，这需要在各个独立的操作系统之间进行任务调度。

编程模型：云计算需要有一种特殊的编程模式，能够把云计算能力封装成标准的Web Services。在这种编程环境下，大的计算任务被映像为多个细小的可计算单元，通过云节点处理后再归约为最终的计算结果。

试题二　论无线网络中的安全问题及防范技术

随着网络技术的飞速发展和普及，无线网络也逐步发展起来，近年来，无线网络已经成为网络扩展的一种重要方式，人们对无线网络依赖的程度也越来越高。无线网络具有安装简便、可移动性、开放性、高灵活性等特点，这些都为人们带来了极大的方便。但也正是因为这些特点，决定了无线网络面临许多安全问题，这些安全问题迫使技术人员开发了相应的安全防范技术和方法。

请围绕“无线网络中的安全问题及防范技术”论题，依次对以下四个方面进行论述。

1．简要论述无线网络面临的安全问题。

2．详细论述针对无线网络主要安全问题的防范技术。

3．详细论述你参与设计和实施的无线网络项目中采用的安全防范方案。

4．分析和评估你所采用的安全防范方案的效果以及进一步改进的措施。

写作要点

1．对无线网络面临的安全问题的叙述要点：

（1）无线网络的类型

根据网络覆盖范围、传输速率和用途的差异，无线网络大体可分为无线广域网、无线城域网、无线局域网、无线个域网和无线体域网。

从网络拓扑结构角度，无线网络又可分为有中心网络和无中心、自组织网络。

（2）无线网络安全与有线网络安全的区别

无线网络的开放性使得网络更容易受到被动窃听或主动干扰等各种攻击；

无线网络的移动性使得安全管理难度更大；

无线网络动态变化的拓扑结构使得安全方案的实施难度更大；

无线网络传输信号的不稳定性带来无线通信网络及其安全机制的健壮性问题；

无线网络终端设备具有与有线网络终端设备不同的特点。

（3）无线网络面临的主要攻击威胁

WEP 攻击

MAC 地址欺骗

DoS 攻击

AP 口令攻击

伪装 AP 攻击

2．对无线网络主要安全问题的防范技术的论述要点：

（1）访问控制

利用 MAC 地址访问控制和服务区认证 ID（SSID）技术来防止非法的无线设备入侵。由于每台计算机的网卡拥有唯一的 MAC 地址，因此可以使用 MAC 地址过滤的策略来防止非法的地址入侵。SSID 使得只有计算机的 SSID 与无线路由器的 SSID 一致时才能访问，因此可以采用隐蔽 SSID 的方法来拒绝非法访问。

（2）数据加密

数据加密是无线网络安全的基础，对传输的数据进行加密是为了防止其在未授权的情况下数据被泄露、破坏或篡改。各个组织和国家提出了多种解决方案，从开始的 WEP 协议，经历 WPA，到 802.11i 协议，安全技术不断地进步。

（3）端口访问技术（802.1x）控制网络接入

IEEE 802.1x 协议是一种基于端口访问的控制协议，能够实现对局域网设备的安全认

证和授权。

3．叙述自己参与设计和实施的无线网络项目，该项目应有一定的规模，自己在该项目中担任的主要工作应有一定的分量，说明项目中设计的安全方案以及选用该方案的理由。

4．具体讨论在方案实施过程中遇到的问题和解决措施，以及实际运行效果。

试题三 论数字化技术的运用及关键技术

随着网络信息技术的进步和社会信息化程度的不断提高，一个由庞大的网络产业带动，并导致整个经济社会产生巨大变革的数字经济时代已经离我们越来越近。目前，“数字化校园”、“数字企业”、“数字城市”等一系列项目快速上马，在这些项目中，信息的数字化与数字信息的网络传输起着举足轻重的作用。

请围绕“数字化技术的运用及关键技术”论题，依次对以下四个方面进行论述。

1．简要介绍单位具体需求，叙述数字化建设的必要性。

2．叙述数字化建设中整体框架及数字化资源。

3．叙述数字化建设中的网络支撑平台。

4．分析在数字化建设中涉及的关键技术及采用的具体举措。

写作要点

1．对数字化建设的必要性的叙述

从单位具体实际出发，介绍原有资源的组织形式，描述清楚数字化建设的必要性，给单位资源利用带来的好处。

2．数字化建设中整体框架及数字化资源的叙述

（1）描述数字化建设常采用的框架，本单位建设框架的选择及理由；

（2）对那些资源进行了数字化。

3．数字化建设中的网络支撑平台的叙述

（1）描述整体网络架构；

（2）实现资源快速共享采用的主要技术；

（3）数字化资源模块的网络组织形式。

4．涉及的关键技术及采用的具体举措的叙述

（1）在方案实施过程中遇到的问题，采用的关键技术；

（2）关键技术产生的实际运行效果。

第19章　2014下半年网络规划设计师上午试题分析与解答

试题（1）

计算机采用分级存储体系的主要目的是为了__（1）__。

（1）A．解决主存容量不足的问题

B．提高存储器读写可靠性

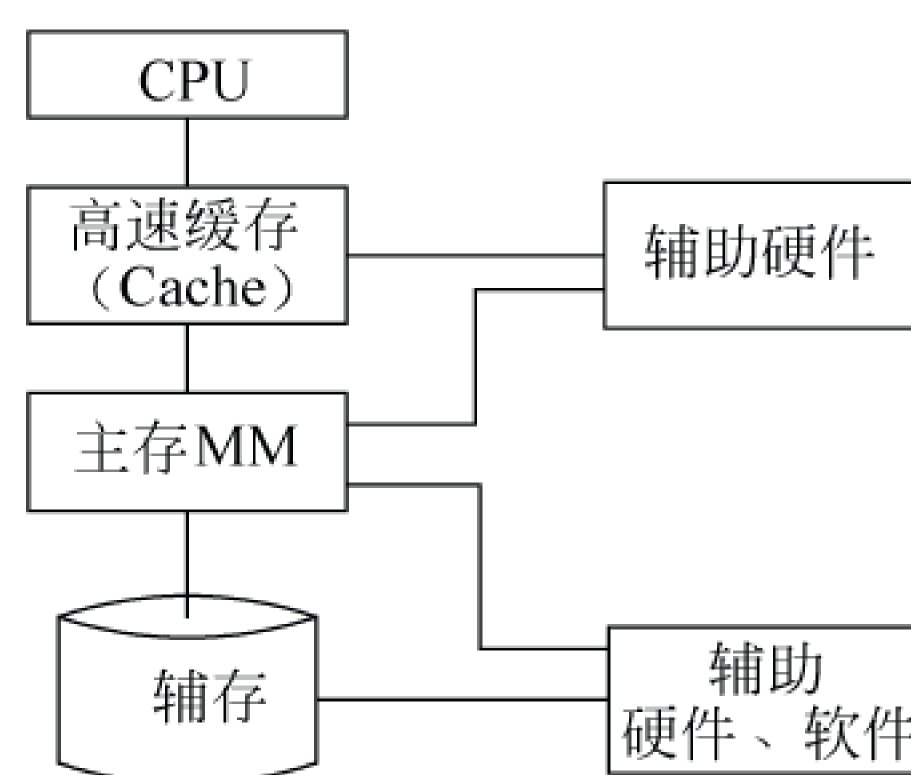
C．提高外设访问效率

D．解决存储的容量、价格和速度之间的矛盾

试题（1）分析

本题考查计算机系统基础知识。

存储体系结构包括不同层次上的存储器，通过适当的硬件、软件有机地组合在一起形成计算机的存储体系结构。例如，由高速缓存（Cache）、主存储器（MM）和辅助存储器构成的3层存储器层次结构存如右图所示。



接近CPU的存储器容量更小、速度更快、成本更高；辅存容量大、速度慢，价格低。采用分级存储体系的目的是解决存储的容量、价格和速度之间的矛盾。

参考答案

（1）D

试题（2）

设关系模式R(U,F)，其中U为属性集，F是U上的一组函数依赖，那么函数依赖的公理系统（Armstrong公理系统）中的合并规则是指__（2）__为F所蕴涵。

（2）A．若A→B，B→C，则A→C

B．若Y⊆X⊆U，则X→Y

C．若A→B，A→C，则A→BC

D．若A→B，C⊆B，则A→C

试题（2）分析

本题考查函数依赖推理规则。

函数依赖的公理系统（即Armstrong公理系统）为：设关系模式R(U,F)，其中U为属性集，F是U上的一组函数依赖，那么有如下推理规则：

A1 自反律：若Y⊆X⊆U，则X→Y为F所蕴涵。

A2 增广律：若X→Y为F所蕴涵，且Z⊆U，则XZ→YZ为F所蕴涵。

A3 传递律：若X→Y，Y→Z为F所蕴涵，则X→Z为F所蕴涵。

根据上述三条推理规则又可推出下述三条推理规则：

A4 合并规则：若 X→Y，X→Z，则 X→YZ 为 F 所蕴涵。

A5 伪传递率：若 X→Y，WY→Z，则 XW→Z 为 F 所蕴涵。

A6 分解规则：若 X→Y，Z⊆Y，则 X→Z 为 F 所蕴涵。

选项 A 符合规则为 A3，即传递规则；选项 B 符合规则为 A1，即为自反规则；选项 C 符合规则为 A4，即为合并规则；选项 D 符合规则为 A6，即为分解规则。

参考答案

（2）C

试题（3）、（4）

在结构化分析方法中，用__（3）__表示功能模型，用__（4）__表示行为模型。

（3）A. ER 图　　B. 用例图　　C. DFD　　D. 对象图

（4）A. 通信图　　B. 顺序图　　C. 活动图　　D. 状态转换图

试题（3）、（4）分析

结构化分析方法的基本思想是自顶向下，逐层分解，把一个大问题分解成若干个小问题，每个小问题再分解成若干个更小的问题。经过逐层分解，每个最低层的问题都是足够简单、容易解决的。结构化方法分析模型的核心是数据字典，围绕这个核心，有三个层次的模型，分别是数据模型、功能模型和行为模型（也称为状态模型）。在实际工作中，一般使用 E-R 图表示数据模型，用 DFD 表示功能模型，用状态转换图表示行为模型。这三个模型有着密切的关系，它们的建立不具有严格的时序性，而是一个迭代的过程。

参考答案

（3）C　　（4）D

试题（5）

以下关于单元测试的方法中，正确的是__（5）__。

（5）A. 驱动模块用来调用被测模块，自顶向下的单元测试中不需要另外编写驱动模块

B. 桩模块用来模拟被测模块所调用的子模块，自顶向下的单元测试中不需要另外编写桩模块

C. 驱动模块用来模拟被测模块所调用的子模块，自底向上的单元测试中不需要另外编写驱动模块

D. 桩模块用来调用被测模块，自底向上的单元测试中不需要另外编写桩模块

试题（5）分析

本题考查单元测试的基本概念。

单元测试也称为模块测试，测试的对象是可独立编译或汇编的程序模块、软件构件或面向对象软件中的类（统称为模块），其目的是检查每个模块能否正确地实现设计说明中的功能、性能、接口和其他设计约束等条件，发现模块内可能存在的各种差错。单元

测试的技术依据是软件详细设计说明书。

测试一个模块时，可能需要为该模块编写一个驱动模块和若干个桩模块。驱动模块用来调用被测模块，它接收测试者提供的测试数据，并把这些数据传送给被测模块，然后从被测模块接收测试结果，并以某种可见的方式将测试结果返回给测试人员；桩模块用来模拟被测模块所调用的子模块，它接受被测模块的调用，检验调用参数，并以尽可能简单的操作模拟被调用的子程序模块功能，把结果送回被测模块。顶层模块测试时不需要驱动模块，底层模块测试时不要桩模块。

单元测试策略主要包括自顶向下的单元测试、自底向上的单元测试、孤立测试和综合测试策略。

① 自顶向下的单元测试。先测试上层模块，再测试下层模块。测试下层模块时由于它的上层模块已测试过，所以不必另外编写驱动模块。

② 自底向上的单元测试。自底向上的单元测试先测试下层模块，再测试上层模块。测试上层模块由于它的下层模块已经测试过，所以不必另外编写桩模块。

③ 孤立测试不需要考虑每个模块与其他模块之间的关系，逐一完成所有模块的测试。由于各模块之间不存在依赖性，单元测试可以并行进行，但因为需要为每个模块单独设计驱动模块和桩模块，增加了额外的测试成本。

④ 综合测试。上述三种单元测试策略各有利弊，实际测试时可以根据软件特点和进度安排情况，将几种测试方法混合使用。

参考答案

（5）A

试题（6）、（7）

某公司欲开发一个用于分布式登录的服务端程序，使用面向连接的 TCP 协议并发地处理多客户端登录请求。用户要求该服务端程序运行在 Linux、Solaris 和 Windows NT 等多种操作系统平台之上，而不同的操作系统的相关 API 函数和数据都有所不同。针对这种情况，公司的架构师决定采用“包装器外观（Wrapper Facade）”架构模式解决操作系统的差异问题。具体来说，服务端程序应该在包装器外观的实例上调用需要的方法，然后将请求和请求的参数发送给__（6）__，调用成功后将结果返回。使用该模式__（7）__。

（6）A．客户端程序　　B．操作系统 API 函数

C．TCP 协议 API 函数　　D．登录连接程序

（7）A．提高了底层代码访问的一致性，但降低了服务端程序的调用性能

B．降低了服务端程序功能调用的灵活性，但提高了服务端程序的调用性能

C．降低了服务端程序的可移植性，但提高了服务端程序的可维护性

D．提高了系统的可复用性，但降低了系统的可配置性

试题（6）、（7）分析

本题主要考查考生对设计模式的理解与应用。

题干描述了某公司欲开发一个用于分布式登录的服务端程序，使用面向连接的 TCP 协议并发地处理多客户端登录请求。用户要求该服务端程序运行在 Linux、Solaris 和 Windows NT 等多种操作系统平台之上，而不同的操作系统的相关 API 函数和数据都有所不同。针对这种情况，公司的架构师决定采用"包装器外观（Wrapper Facade）"架构模式解决操作系统的差异问题。具体来说，服务端程序应该在包装器外观的实例上调用需要的方法，然后将请求和请求的参数发送给操作系统 API 函数，调用成功后将结果返回。使用该模式提高了底层代码访问的一致性，但降低了服务端程序的调用性能。

参考答案

（6）B　　　（7）A

试题（8）

某服装店有甲、乙、丙、丁四个缝制小组。甲组每天能缝制 5 件上衣或 6 条裤子；乙组每天能缝制 6 件上衣或 7 条裤子；丙组每天能缝制 7 件上衣或 8 条裤子；丁组每天能缝制 8 件上衣或 9 条裤子。每组每天要么缝制上衣，要么缝制裤子，不能弄混。订单要求上衣和裤子必须配套（每套衣服包括一件上衣和一条裤子）。只要做好合理安排，该服装店 15 天最多能缝制__（8）__套衣服。

（8）A. 208　　B. 209　　C. 210　　D. 211

试题（8）分析

本题考查数学应用能力。

根据题意，甲、乙、丙、丁四组做上衣和裤子的效率之比分别为 5/6、6/7、7/8、8/9，并且依次增加。因此，丁组做上衣效率更高，甲组做裤子效率更高。为此，安排甲组 15 天全做裤子，丁组 15 天全做上衣。

设乙组用 x 天做上衣，15-x 天做裤子；丙组用 y 天做上衣，15-y 天做裤子，为使上衣和裤子配套，则有

$$0+6x+7y+8*15=6*15+7(15-x)+8(15-y)+0$$

所以，13x+15y=13*15，y=13-13x/15

15 天共做套数 6x+7y+8*15=6x+7(13-13x/15)+120=211-x/15

只有在 x=0 时，最多可做 211 套。

此时，y=13，即甲乙丙丁四组分别用 0、0、13、15 天做上衣，用 15、15、2、0 天做裤子。

参考答案

（8）D

试题（9）

生产某种产品有两个建厂方案：（1）建大厂，需要初期投资 500 万元。如果产品销路好，每年可以获利 200 万元；如果销路不好，每年会亏损 20 万元。（2）建小厂，需要初期投资 200 万元。如果产品销路好，每年可以获利 100 万元；如果销路不好，每年只

能获利 20 万元。

市场调研表明，未来 2 年，这种产品销路好的概率为 70%。如果这 2 年销路好，则后续 5 年销路好的概率上升为 80%；如果这 2 年销路不好，则后续 5 年销路好的概率仅为 10%。为取得 7 年最大总收益，决策者应＿（9）＿。

（9）A．建大厂，总收益超 500 万元　　B．建大厂，总收益略多于 300 万元

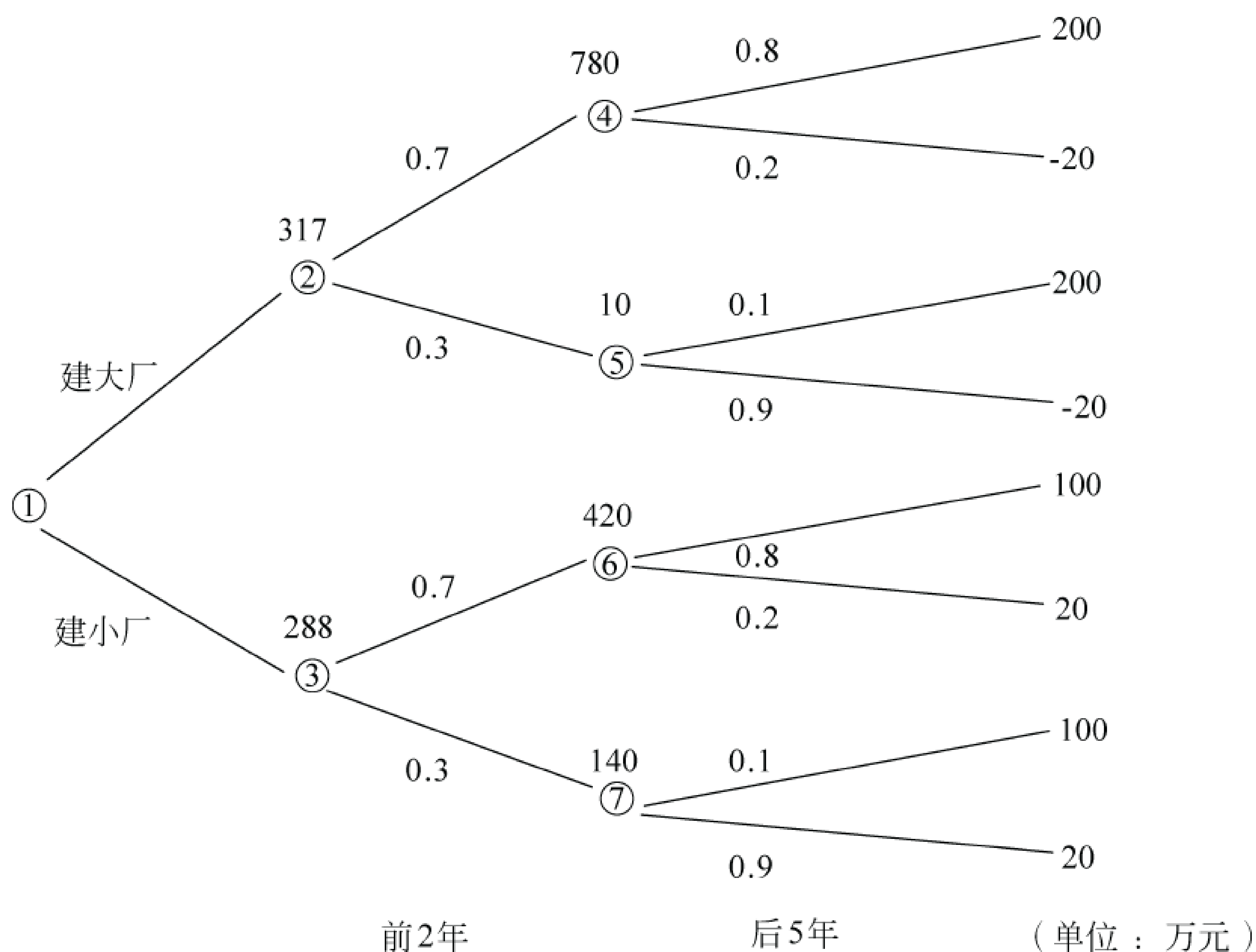
C．建小厂，总收益超 500 万元　　D．建小厂，总收益略多于 300 万元

试题（9）分析

本题考查数学应用能力。

采用决策树分析方法解答如下：

先画决策树，从左至右逐步画出各个决策分支，并在各分支上标出概率值，再在最右端分别标出年获利值。然后，从右至左，计算并填写各节点处的期望收益。



在右面四个节点处依次按下列算式计算 5 年的期望值，并将结果分别写在节点处。

节点④:　{200*0.8+(-20)*0.2}*5=780

节点⑤:　{200*0.1+(-20}*0.9)*5=10

节点⑥:　{100*0.8+20*0.2}*5=420

接点⑦:　{100*0.1+20*0.9}*5=140

再在②、③节点处按如下算式计算 2 年的期望值（扣除投资额），并将结果（7 年总收益）写在节点处。

节点②：{200*0.7+(-20)*0.3}*2+{780*0.7+10*0.3}-500=317

节点③：{100*0.7+20*0.3}*2+{420*0.7+140*0.3}-200=288

由于节点②处的总收益值大于节点③处的总收益值。因此决定建大厂。

参考答案

（9）B

试题（10）

软件商标权的保护对象是指__（10）__。

（10）A. 商业软件　　B. 软件商标

C. 软件注册商标　　D. 已使用的软件商标

试题（10）分析

软件商标权是软件商标所有人依法对其商标（软件产品专用标识）所享有的专有使用权。在我国，商标权的取得实行的是注册原则，即商标所有人只有依法将自己的商标注册后，商标注册人才能取得商标权，其商标才能得到法律的保护。对其软件产品已经冠以商品专用标识，但未进行商标注册，没有取得商标专用权，此时该软件产品专用标识就不能得到商标法的保护，即不属于软件商标权的保护对象。未注册商标可以自行在商业经营活动中使用，但不受法律保护。未注册商标不受法律保护，不等于对使用未注册商标行为放任自流。为了更好地保护注册商标的专用权和维护商标使用的秩序，需要对未注册商标的使用加以规范。所以《商标法》第四十八条专门对使用未注册商标行为做了规定。未注册商标使用人不能违反此条规定，否则商标行政主管机关将依法予以查处。

参考答案

（10）C

试题（11）、（12）

基于模拟通信的窄带 ISDN 能够提供声音、视频、数据等传输服务。ISDN 有两种不同类型的信道，其中用于传送信令的是__（11）__，用于传输语音/数据信息的是__（12）__。

（11）A. A 信道　　B. B 信道　　C. C 信道　　D. D 信道

（12）A. A 信道　　B. B 信道　　C. C 信道　　D. D 信道

试题（11）、（12）分析

ISDN 分为窄带 ISDN（Narrowband ISDN，N-ISDN）和宽带 ISDN（Broadband ISDN，B-ISDN）。窄带 ISDN 的目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一个网络上统一传输。窄带 ISDN 系统提供两种用户接口：即基本速率接口 2B+D 和基群速率接口 30B+D。其中的 B 信道是 64kb/s 的话音或数据信道，而 D 信道是 16kb/s 或 64kb/s 的信令信道。对于家庭用户，通信公司在用户住所安装一个第一类网络终接设备 NT1。用户可以在连接 NT1 的总线上最多挂接 8 台设备，共享 2B+D 的 144kb/s 信道。大型商业用户则要通过第二类网络终接设备 NT2 连接 ISDN，这种接入方式可以提供 30B+D（2.048Mb/s）的接口速率。

参考答案

（11）D　　（12）B

试题（13）

下面关于帧中继的描述中，错误的是__（13）__。

（13）A．帧中继在第三层建立固定虚电路和交换虚电路

B．帧中继提供面向连接的服务

C．帧中继可以有效地处理突发数据流量

D．帧中继充分地利用了光纤通信和数字网络技术的优势

试题（13）分析

帧中继（Frame Relay，FR）网络运行在 OSI 参考模型的物理层和数据链路层。FR 用第二层协议数据单元帧来承载数据业务，因而第三层被省掉了。帧中继提供面向连接的服务，在互相通信的每对设备之间都存在一条定义好的虚电路，并且指定了一个链路识别码 DLCI。帧中继利用了光纤通信和数字网络技术的优势，FR 帧层操作比 HDLC 简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。所以，帧中继比 X.25 具有更高的传输效率。

参考答案

（13）A

试题（14）、（15）

海明码是一种纠错编码，一对有效码字之间的海明距离是__（14）__。如果信息为 10 位，要求纠正 1 位错，按照海明编码规则，需要增加的校验位是__（15）__位。

（14）A．两个码字的比特数之和　　B．两个码字的比特数之差

C．两个码字之间相同的比特数　　D．两个码字之间不同的比特数

（15）A．3　　B．4　　C．5　　D．6。

试题（14）、（15）分析

海明（Hamming）研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字。码字之间的海明距离是一个码字要变成另一个码字时必须改变的最小位数。例如，7 位 ASCII 码增加一位奇偶位成为 8 位的码字，这 128 个 8 位的码字之间的海明距离是 2。所以当其中 1 位出错时便能检测出来。两位出错时就变成另外一个有效码字了。

按照海明的理论，纠错编码就是要把所有合法的码字尽量安排在 n 维超立方体的顶点上。使得任一对码字之间的距离尽可能大。如果任意两个码字之间的海明距离是 d，则所有少于等于 d-1 位的错误都可以被检查出来，所有少于 d/2 位的错误都可以被纠正。一个自然的推论是，对某种长度的错误串，要纠正它就要用比仅仅检测它多一倍的冗余位。

如果对于 m 位的数据，增加 k 位冗余位，则组成 n=m+k 位的纠错码。对于 2^m 个有

效码字中的任意一个，都有 n 个无效但可以纠错的码字。这些可纠错的码字与有效码字的距离是 1，含单个错误位。这样，对于一个有效码字总共有 n+1 个可识别的码字。这 n+1 个码字相对于其他 2^m-1 个有效码字的距离都大于 1。这意味着总共有 2^m (n+1)个有效的或是可纠错的码字。显然这个数应小于等于码字的所有可能的个数 2^n。于是，我们有

$$2^m (n+1) < 2^n$$

因为 n=m+k，我们得出

$$M+k+1 < 2^k$$

对于给定的数据位 m，上式给出了 k 的下界，即要纠正单个错误，k 是必须取的最小值。本题中由于 m=10，所以得到 k=4。

参考答案

（14）D　　（15）B

试题（16）、（17）

PPP 的认证协议 CHAP 是一种__（16）__的安全认证协议，发起挑战的应该是__（17）__。

（16）A. 一次握手　　B. 两次握手　　C. 三次握手　　D. 同时握手

（17）A. 连接方　　B. 被连接方　　C. 任意一方　　D. 第三方

试题（16）、（17）分析

PPP 支持的质询握手认证协议（Challenge Handshake Authentication Protocol，CHAP）采用三次握手方式周期地验证对方的身份。首先是逻辑链路建立后认证服务器（被连接方）就要发送一个挑战报文（随机数），终端计算该报文的 Hash 值并把结果返回服务器。然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较，如果匹配，则认证通过，连接得以建立，否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与，而密钥是不通过网络传送的，所以 CHAP 是很安全的认证机制。在后续的通信过程中，每经过一个随机的间隔，这个认证过程都可能被重复，以缩短入侵者进行持续攻击的时间。值得注意的是，这种方法可以进行双向身份认证，终端也可以向服务器进行挑战，使得双方都能确认对方身份的合法性。

参考答案

（16）C　　（17）B

试题（18）

关于无线网络中的直接序列扩频技术，下面描述中错误的是__（18）__。

（18）A. 用不同的频率传播信号扩大了通信的范围

B. 扩频通信减少了干扰并有利于通信保密

C. 每一个信号比特可以用 N 个码片比特来传输

D. 信号散布到更宽的频带上降低了信道阻塞的概率

试题（18）分析

在直接序列扩频方案中，信号源中的每一比特用称为码片的 N 个比特来传输，这个过程在扩展器中进行。然后把所有的码片用传统的数字调制器发送出去。在接收端，收到的码片解调后被送到一个相关器，自相关函数的尖峰用于检测发送的比特。好的随机码相关函数具有非常高的尖峰/旁瓣比，如下图所示。数字系统的带宽与其所采用的脉冲信号的持续时间成反比。在 DSSS 系统中，由于发射的码片只占数据比特的 1/N，所以 DSSS 信号的带宽是原来数据带宽的 N 倍。

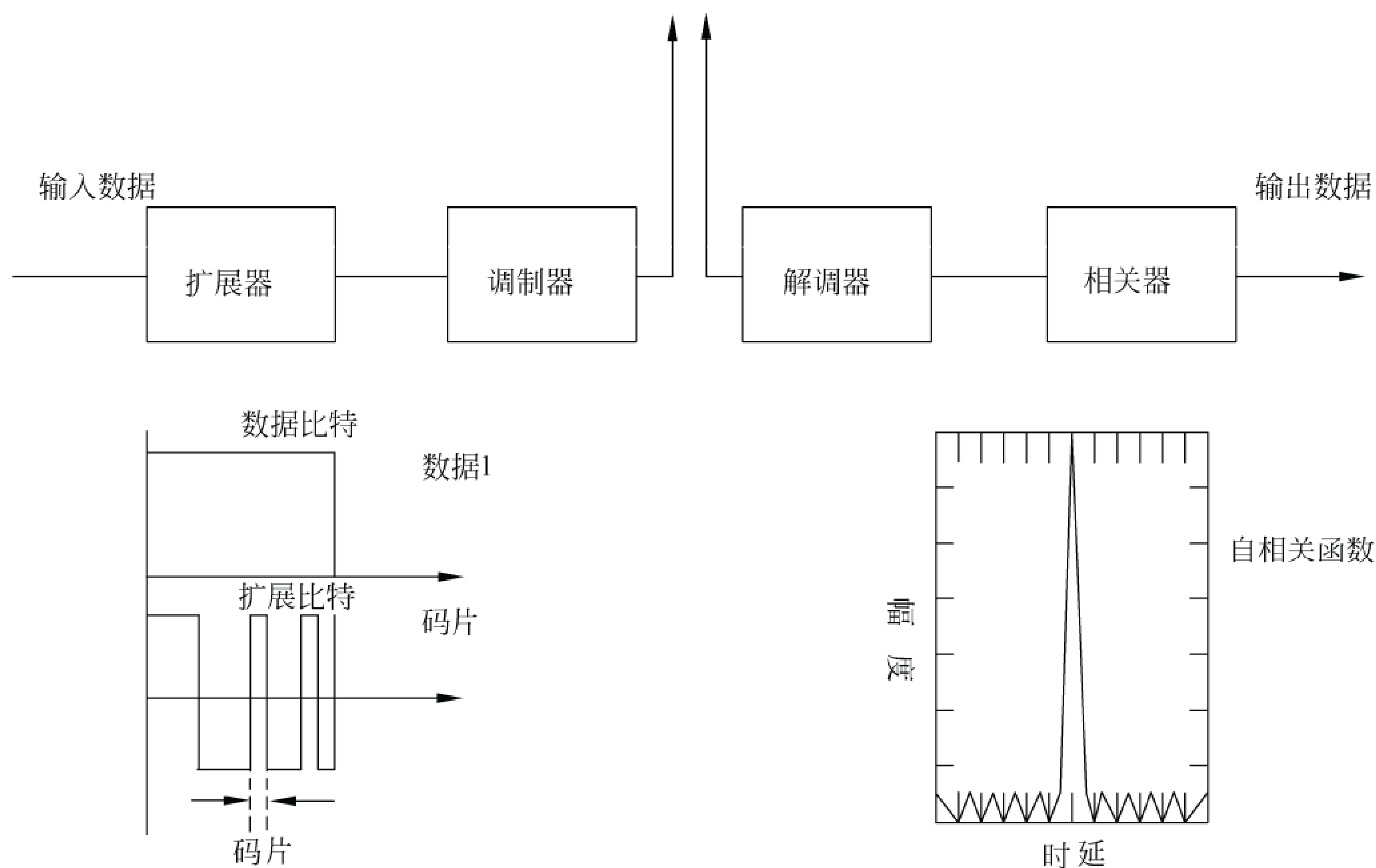


图　DSSS 的频谱扩展器和自相关检测器

在 DSSS 扩频通信中，每一个信号比特用 N 个比特的码片来传输，这样使得信号散布到更宽的频带上，降低了信道阻塞的概率，减少了干扰并有利于通信保密。

参考答案

（18）A

试题（19）

IETF 定义的集成服务（IntServ）把 Internet 服务分成了三种服务质量不同的类型，这三种服务不包括<u>（19）</u>。

（19）A．保证质量的服务：对带宽、时延、抖动和丢包率提供定量的保证

B．尽力而为的服务：这是一般的 Internet 服务，不保证服务质量

C．负载受控的服务：提供类似于网络欠载时的服务，定性地提供质量保证

D．突发式服务：如果有富余的带宽，网络保证满足服务质量的需求

试题（19）分析

IETF 集成服务（IntServ）工作组根据服务质量的不同，把 Internet 服务分成了三种类型：

① 保证质量的服务（Guranteed Services）：对带宽、时延、抖动和丢包率提供定量的保证；

② 负载受控的服务（Controlled-load Services）：提供一种类似于网络欠载情况下的服务，这是一种定性的指标；

③ 尽力而为的服务（Best-Effort）：这是 Internet 提供的一般服务，基本上无任何质量保证。

参考答案

（19）D

试题（20）

按照网络分层设计模型，通常把局域网设计为 3 层，即核心层、汇聚层和接入层，以下关于分层网络功能的描述中，不正确的是 __（20）__ 。

（20）A．核心层设备负责数据包过滤、策略路由等功能

B．汇聚层完成路由汇总和协议转换功能

C．接入层应提供一部分管理功能，例如 MAC 地址认证、计费管理等

D．接入层要负责收集用户信息，例如用户 IP 地址、MAC 地址、访问日志等

试题（20）分析

三层模型将大型局域网划分为核心层、汇聚层和接入层。每一层都有特定的作用。

① 核心层是因特网络的高速骨干网，由于其重要性，因此在设计中应该采用冗余组件设计。在设计核心层设备的功能时，应尽量避免使用数据包过滤和策略路由等降低数据包转发速率的功能。如果需要连接因特网和外部网络，核心层还应包括一条或多条连接到外部网络的连接。

② 汇聚层是核心层和接入层之间的分界点，应尽量将资源访问控制、流量的控制等在汇聚层实现。为保证层次化的特性，汇聚层应该向核心层隐藏接入层的细节，例如不管接入层划分了多少个子网，汇聚层向核心层路由器进行路由宣告时，仅宣告由多个子网地址汇聚而成的网络。为保证核心层能够连接运行不同协议的区域网络，各种协议的转换都应在汇聚层完成。

③ 接入层为用户提供在本地网段访问应用系统的能力，也要为相邻用户之间的互访需求提供足够的带宽。接入层还应该负责一些用户管理功能，以及用户信息的收集工作。

参考答案

（20）A

试题（21）、（22）

配置路由器有多种方法，一种方法是通过路由器 console 端口连接 __（21）__ 进行配

置，另一种方法是通过 TELNET 协议连接＿(22)＿进行配置。

（21）A．中继器　　B．AUX 接口　　C．终端　　D．TCP/IP 网络

（22）A．中继器　　B．AUX 接口　　C．终端　　D．TCP/IP 网络

试题（21）、（22）分析

对路由器进行初始配置时，要用工作电缆连接仿真终端和路由器的 Console 端口。当路由器部署在网络中时，可以在终端上运行 TELNET 协议，通过 TCP/IP 网络登录到路由器，再在终端上键入配置命令，对路由器进行配置。

参考答案

（21）C　　（22）D

试题（23）

如果允许来自子网 172.30.16.0/24 到 172.30.31.0/24 的分组通过路由器，则对应 ACL 语句应该是＿(23)＿。

（23）A．access-list 10 permit 172.30.16.0 255.255.0.0

B．access-list 10 permit 172.30.16.0 0.0.255.255

C．access-list 10 permit 172.30.16.0 0.0.15.255

D．access-list 10 permit 172.30.16.0 255.255.240.0

试题（23）分析

如果允许来自子网 172.30.16.0/24 到 172.30.31.0/24 的分组通过路由器，则对应的 ACL 语句应该是 access-list 10 permit 172.30.16.0 0.0.15.255。值得注意的是反掩码 0.0.15.255 正好覆盖了 172.30.16.0 网络中最后 12 位表示的全部地址。

参考答案

（23）C

试题（24）

结构化布线系统分为六个子系统，其中水平子系统＿(24)＿。

（24）A．由各种交叉连接设备以及集线器和交换机等交换设备组成

B．连接干线子系统和工作区子系统

C．由终端设备到信息插座的整个区域组成

D．实现各楼层设备间子系统之间的互连

试题（24）分析

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、管理子系统、干线（或垂直）子系统、设备间子系统和建筑群子系统。其中水平子系统是指各个楼层接线间的配线架到工作区信息插座之间所安装的线缆系统，其作用是将干线子系统与用户工作区连接起来。

参考答案

（24）B

试题（25）

边界网关协议 BGP4 被称为路径矢量协议，它传送的路由信息是由一个地址前缀后跟 (25) 组成。

（25）A．一串 IP 地址　　　　B．一串自治系统编号
　　　C．一串路由器编号　　　D．一串子网地址

试题（25）分析

边界网关协议 BGP 是应用于自治系统（AS）之间的外部网关协议。BGP4 基本上是一个距离矢量路由协议，但是与 RIP 协议采用的算法稍有区别。BGP 不但为每个目标计算最小通信费用，而且跟踪通向目标的路径。它不但把目标的通信费用发送给每一个邻居，而且也公告通向目标的最短路径（由地址前缀后跟一串自治系统编号组成）。所以 BGP4 被称为路径矢量协议。

参考答案

（25）B

试题（26）

与 RIPv2 相比，IGRP 协议增加了一些新的特性，下面的描述中错误的是 (26) 。

（26）A．路由度量不再把跳步数作为唯一因素，还包含了带宽、延迟等参数
　　　B．增加了触发更新来加快路由收敛，不必等待更新周期结束再发送更新报文
　　　C．不但支持相等费用通路负载均衡，而且支持不等费用通路的负载均衡
　　　D．最大跳步数由 15 跳扩大到 255 跳，可以支持更大的网络

试题（26）分析

内部网关路由协议（Interior Gateway Routing Protocol，IGRP）是 Cisco 公司 1980 年代设计的一种动态距离矢量路由协议。它组合了网络配置的各种因素，包括带宽、延迟、可靠性和负载等作为路由度量。它支持相等费用通路负载均衡和不等费用通路负载均衡。IGRP 的最大跳步数由 15 跳扩大到 255 跳，可以支持比 RIPv2 更大的网络。

默认情况下，IGRP 每 90s 发送一次路由更新广播，在 3 个更新周期内（即 270s）没有从某个路由器接收到更新报文，则宣布该路由不可访问。在 7 个更新周期即 630s 后，IOS 从路由表中清除该路由表项。

用触发更新来加快路由收敛，这是 RIPv2 和 IGRP 都有的功能。

参考答案

（26）B

试题（27）、（28）

城域以太网在各个用户以太网之间建立多点的第二层连接，IEEE 802.1ad 定义的运营商网桥协议提供的基本技术是在以太帧中插入 (27) 字段，这种技术被称为 (28) 技术。

（27）A．运营商 VLAN 标记　　　　B．运营商虚电路标识

C. 用户 VLAN 标记　　D. 用户帧类型标记

（28）A. Q-in-Q　　B. IP-in-IP

C. NAT-in-NAT　　D. MAC-in-MAC

试题（27）、（28）分析

城域以太网论坛（Metro Ethernet Forum，MEF）是由网络设备制造商和网络运营商组成的非盈利组织，专门从事城域以太网的标准化工作。MEF 定义的 E-LAN 服务的基本技术是 802.1q 的 VLAN 帧标记。假定各个用户的以太网称为 C-网，运营商建立的城域以太网称为 S-网。如果不同 C-网中的用户要进行通信，以太帧在进入用户网络接口（User-Network Interface，UNI）时被插入一个 S-VID（Server Provider-VLAN ID）字段，用于标识 S-网中的传输服务，而用户的 VLAN 帧标记（C-VID）则保持不变，当以太帧到达目标 C-网时，S-VID 字段被删除，如下图所示。这样就解决了两个用户以太网之间透明的数据传输问题。这种技术定义在 IEEE 802.1ad 的运营商网桥协议（Provider Bridge Protocol）中，被称为 Q-in-Q 技术。

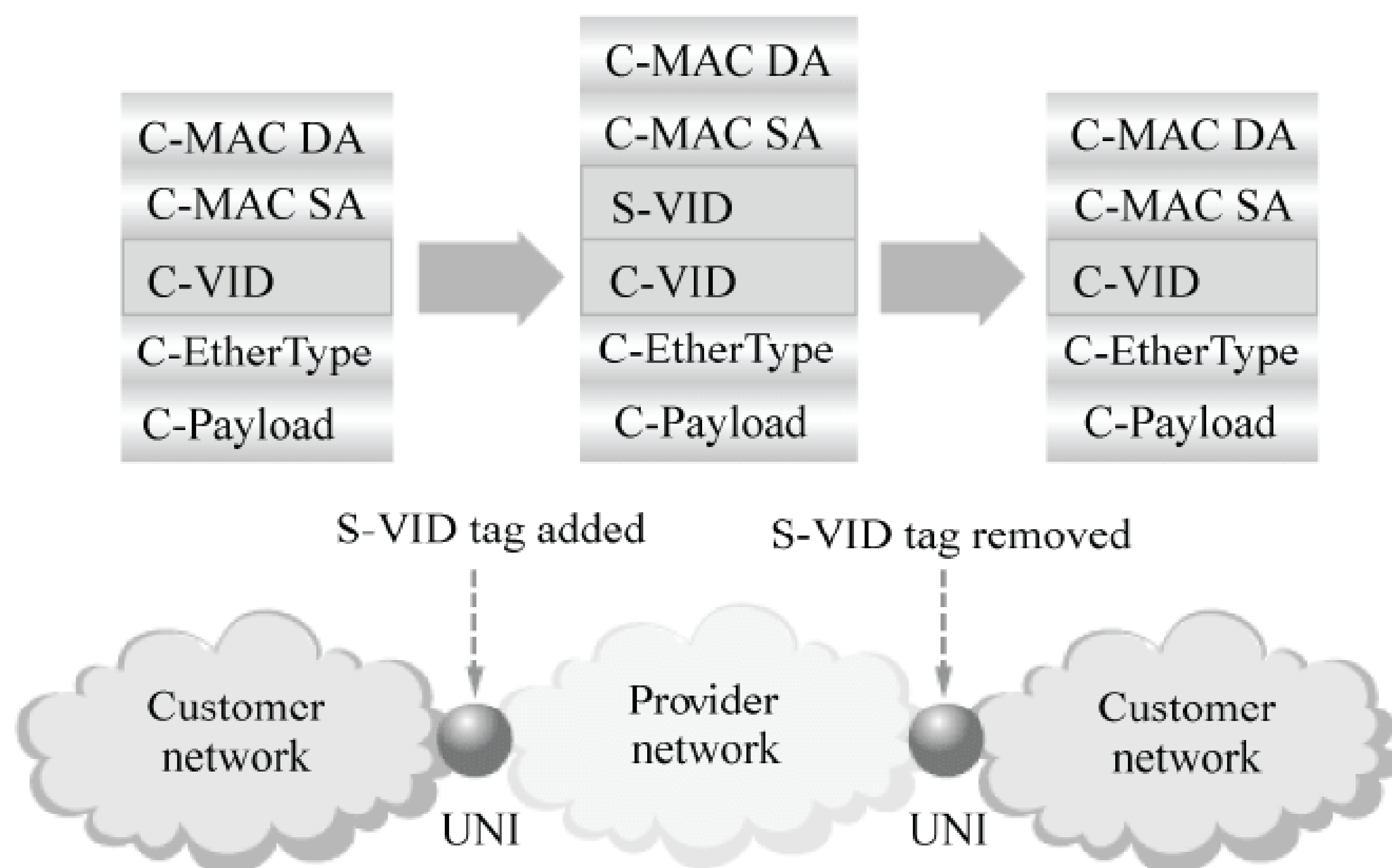


图　802.1ad 的帧格式

Q-in-Q 实际上是把用户 VLAN 嵌套在城域以太网的 VLAN 中传送，由于其简单性和有效性而得到电信运营商的青睐。但是这样一来，所有用户的 MAC 地址在城域以太网中都是可见的，任何 C-网的改变都会影响到 S-网的配置，增加了管理的难度。而且 S-VID 字段只有 12 位，只能标识 4096 个不同的传输服务，网络的可扩展性也受到限制。从用户角度看，网络用户的 MAC 地址都暴露在整个城域以太网中，使得网络的安全性受到威胁。

参考答案

（27）A　　（28）A

试题（29）

数据传输时会存在各种时延，路由器在报文转发过程中产生的时延不包括（29）。

（29）A．排队时延 B．TCP 流控时延
C．路由计算时延 D．数据包处理时延

试题（29）分析

本题考查路由器的工作原理。

路由器在接收到报文后，先在输入链路进行排队，然后进行检验，计算路由，加入到输出链路进行转发。

参考答案

（29）B

试题（30）、（31）

某用户为了保障信息的安全，需要对传送的信息进行签名和加密，考虑加解密时的效率与实现的复杂性，加密时合理的算法是（30），签名时合理的算法为（31）。

（30）A．MD5 B．RC-5 C．RSA D．ECC
（31）A．RSA B．SHA-1 C．3DES D．RC-5

试题（30）、（31）分析

本题考查加密和签名算法。

考虑加解密时的效率与实现的复杂性，通常采用对称密钥加密算法对数据进行加密，采用公钥算法进行签名。SHA-1 和 MD5 属于摘要算法，3DES 和 RC-5 属于对称密钥加密算法，ECC 和 RSA 是公钥算法。

参考答案

（30）B （31）A

试题（32）

某单位采用 DHCP 进行 IP 地址自动分配，用户收到（32）消息后方可使用其中分配的 IP 地址。

（32）A．DhcpDiscover B．DhcpOffer
C．DhcpNack D．DhcpAck

试题（32）分析

本题考查 DHCP 协议的工作原理。

当用户初始启动时发送 DhcpDiscover 报文请求 IP 地址；如果有服务器进行响应，发送 DhcpOffer 报文；若用户采用某服务器提供的 IP 地址，采用 DhcpRequest 报文进行请求；服务器在接收到报文后，采用 DhcpAck 报文进行确认，用户收到报文后就可以采用服务器提供的 IP 地址了。

参考答案

（32）D

试题（33）

DNS 服务器中提供了多种资源记录，其中（33）定义了域名的反向查询。

（33）A．SOA　　B．NS　　C．PTR　　D．MX

试题（33）分析

本题考查 DNS 服务器中的资源记录。

DNS 服务器中提供了多种资源记录，其中类型 SOA 查询的是授权域名服务器；NS 查询的是域名；PTR 是依据 IP 查域名，即域名的反向查询；MX 是邮件服务器记录。

参考答案

（33）C

试题（34）

IIS 服务支持多种身份验证，其中＿（34）＿提供的安全功能最低。

（34）A．.NET Passport 身份验证　　B．集成 Windows 身份验证

C．基本身份验证　　D．摘要式身份验证

试题（34）分析

本题考查 IIS 模块中身份验证相关问题。

基本身份验证采用明文形式对用户名和口令进行传送和验证，安全级别最低。

参考答案

（34）C

试题（35）、（36）

Windows 中的 Netstat 命令显示有关协议的统计信息。下图中显示列表第二列 Local Address 显示的是＿（35）＿。当 TCP 连接处于 SYN_SENT 状态时，表示＿（36）＿。

```
C:\Documents and Settings\Administrator>netstat  -o 4

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1172   121.11.159.208:http    SYN_SENT        1572

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1173   121.11.159.208:http    SYN_SENT        1572

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1173   121.11.159.208:http    SYN_SENT        1572

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1176   124.115.3.126:http     ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1178   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1179   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1180   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1182   124.115.3.126:http     ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1183   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1184   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1185   222.73.73.173:http     ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1186   222.73.78.14:http      SYN_SENT        3096
```

（35）A．本地计算机的 IP 地址和端口号

B．本地计算机的名字和进程 ID
C．本地计算机的名字和端口号
D．本地计算机的 MAC 地址和进程 ID

（36）A．已经发出了连接请求
B．连接已经建立
C．处于连接监听状态
D．等待对方的释放连接响应

试题（35）、（36）分析

本题考查网络管理命令及 TCP 三次握手建立连接状态。

在 Windows 操作系统中，采用命令 Netstat 来显示本机 Internet 应用的统计信息。其中 Local Address 显示的是本地主机的名称及 TCP 连接或 UDP 所采用的端口号。

当 TCP 连接处于 SYN_SENT 状态时，表示已经发出了连接请求，等待对方握手信号；处于连接监听状态是对方被动打开，等待连接建立请求，状态为 LISTEN；连接已经建立状态是 ESTABLISHED；等待对方的释放连接响应状态是 FIN-WAIT-1。

参考答案

（35）C （36）A

试题（37）

设有下面 4 条路由：210.114.129.0/24、210.114.130.0/24、210.114.132.0/24 和 210.114.133.0/24，如果进行路由汇聚，能覆盖这 4 条路由的地址是 （37） 。

（37）A．210.114.128.0/21 B．210.114.128.0/22
C．210.114.130.0/22 D．210.114.132.0/20

试题（37）分析

展开 IP 地址的第 3 字节如下：

第 1 条路由：10000001
第 2 条路由：10000010
第 3 条路由：10000100
第 4 条路由：10000101

聚合之后该字节前 5 比特网络号，后 3 比特主机号，即网络号 210.114.128.0，掩码长度 21 位。

参考答案

（37）A

试题（38）

下面的地址中属于单播地址的是 （38） 。

（38）A．125.221.191.255/18 B．192.168.24.123/30
C．200.114.207.94/27 D．224.0.0.23/16

试题（38）分析

下面 4 个网络地址的二进制形式是

A．125.221.191.255/18　　**01111101 .11011101 .10**111111.11111111

B．192.168.24.123/30　　**11000000.10101000.00011000.011110**11

C．200.114.207.94/27　　**11001000.01110010.11001111.010**11110

D．224.0.0.23/16　　**11100000.00000000**.00000000.00010111

上面各地址二进制表示中的加黑部分是子网掩码，可以看出 A 和 B 都是广播地址，D 是组播地址，只有 C 是单播主机地址。

参考答案

（38）C

试题（39）

IP 地址 202.117.17.255/22 是什么地址？__（39）__。

（39）A．网络地址　　B．全局广播地址

C．主机地址　　D．定向广播地址

试题（39）分析

IP 地址 202.117.17.255/22 的二进制形式是 **11001010.01110101.000100**01.11111111，其中的网络号是 **11001010.01110101.000100**，主机号是 01.11111111。

参考答案

（39）C

试题（40）

IPv6 地址的格式前缀用于表示地址类型或子网地址，例如 60 位的地址前缀 10DE00000000CD3 有多种合法的表示形式，下面的选项中，不合法的是__（40）__。

（40）A．10DE:0000:0000:CD30:0000:0000:0000:0000/60

B．10DE::CD30:0:0:0:0/60

C．10DE:0:0:CD3/60

D．10DE:0:0:CD30::/60

试题（40）分析

以上 IPv6 地址前缀中不合法的是 10DE:0:0:CD3/60，因为这种表示可展开为 10DE:0000:0000:0000:0000:0000:0000:0CD3，另外 CD30 也变成了 0CD3，这些都是错误的。

参考答案

（40）C

试题（41）

下列攻击方式中，__（41）__不是利用 TCP/IP 漏洞发起的攻击。

（41）A．SQL 注入攻击　　B．Land 攻击

C．Ping of Death　　D．Teardrop 攻击

试题（41）分析

本题考查网络安全攻击的基础知识。

SQL 注入攻击是指用户通过提交一段数据库查询代码，根据程序返回的结果，获得攻击者想要的数据，这就是所谓的 SQL Injection，即 SQL 注入攻击。这种攻击方式是通过对数据库查询代码和返回结果的分析而实现的。

Land 攻击是指攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过 IP 欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能。

Ping of Death 攻击是攻击者向被攻击者发送一个超过 65536 字节的数据包 ping 包，由于接收者无法处理这么大的 ping 包而造成被攻击者系统崩溃、挂机或重启。

Teardrop 攻击就是利用 IP 包的分段/重组技术在系统实现中的一个错误，即在组装 IP 包时只检查了每段数据是否过长，而没有检查包中有效数据的长度是否过小，当数据包中有效数据长度为负值时，系统会分配一个巨大的存储空间，这样的分配会导致系统资源大量消耗，直至重新启动。

通过以上解释，可见，Land 攻击、Ping of Death 攻击和 Teardrop 攻击均是利用 TCP/IP 的漏洞所发起的攻击。

参考答案

（41）A

试题（42）

下列安全协议中__（42）__是应用层安全协议。

（42）A．IPSec　　B．L2TP　　C．PAP　　D．HTTPS

试题（42）分析

本题考查网络安全协议的基础知识。

IPSec 是 IETF 制定的 IP 层加密协议，PKI 技术为其提供了加密和认证过程的密钥管理功能。IPSec 主要用于开发新一代的 VPN。

L2TP 是一种二层协议主要是对传统拨号协议 PPP 的扩展，通过定义多协议跨越第二层点对点链接的一个封装机制，来整合多协议拨号服务至现有的因特网服务提供商点，保证分散的远程客户端通过隧道方式经由 Internet 等网络访问企业内部网络。

PAP 协议是二层协议 PPP 协议的一种握手协议，以保证 PPP 链接安全性。

HTTPS 是一个安全通信通道，用于在客户计算机和服务器之间交换信息。它使用安全套接字层（SSL）进行信息交换，所有的数据在传输过程中都是加密的。

参考答案

（42）D

试题（43）

某网络管理员在园区网规划时，在防火墙上启用了 NAT，以下说法中错误的是 （43） 。

（43）A．NAT 为园区网内用户提供地址翻译和转换，以使其可以访问互联网
B．NAT 为 DMZ 区的应用服务器提供动态的地址翻译和转换，使其能访问外网
C．NAT 可以隐藏内部网络结构以保护内部网络安全
D．NAT 支持一对多和多对多的地址翻译和转换

试题（43）分析

本题考查防火墙功能的知识。

NAT（Network Address Translation）叫做网络地址翻译，或者网络地址转换，它的主要功能是对使用似有地址内部网络用户提供 Internet 接入的方式，将私有地址固定地转换为公有地址以访问互联网，NAT 支持一对多和多对多的地址转换方式。由于通过 NAT 访问互联网的用户经过了地址翻译/转换，并非使用原地址访问互联网，因此外部网络对内网的地址结构是不得而知的，依此形成了对内部网络的隐藏和保护。

不能对内部网络中服务器使用 NAT 进行地址转换或者地址翻译，否则，用户将无法联系到内部网络的服务器。

参考答案

（43）B

试题（44）

在 SET 协议中，默认使用 （44） 对称加密算法。

（44）A．IDEA　　B．RC5　　C．三重 DES　　D．DES

试题（44）分析

本题考查安全支付协议的知识。

SET 协议是 PKI 框架下的一个典型实现。安全核心技术主要有公开密钥加密、数字签名、数字信封、消息摘要、数字证书等，主要应用于 B2C 模式中保障支付信息的安全性。SET 协议使用密码技术来保障交易的安全，主要包括散列函数、对称加密算法和非对称加密算法等。SET 中默认使用的散列函数是 SHA，对称密码算法则通常采用 DES，公钥密码算法一般采用 RSA。

参考答案

（44）D

试题（45）～（47）

2013 年 6 月，WiFi 联盟正式发布 IEEE 802.11ac 无线标准认证。802.11ac 是 802.11n 的继承者，新标准的理论传输速度最高可达到 1Gbps。它采用并扩展了源自 802.11n 的空中接口概念，其中包括：更宽的 RF 带宽，最高可提升至 （45） ；更多的 MIMO 空间流，最多增加到 （46） 个；多用户的 MIMO，以及更高阶的调制，最大达到

（47）____。

（45）A．40MHz　　B．80MHz　　C．160MHz　　D．240MHz

（46）A．2　　B．4　　C．8　　D．16

（47）A．16QAM　　B．64QAM　　C．128QAM　　D．256QAM

试题（45）～（47）分析

本题考查新的 802.11ac 无线标准认证。IEEE 802.11ac，是一个 802.11 无线局域网（WLAN）通信标准，它通过 5GHz 频带（也是其得名原因）进行通信。理论上，它能够提供最少 1Gbps 带宽进行多站式无线局域网通信，或是最少 500Mbps 的单一连接传输带宽。802.11ac 是 802.11n 的继承者。它采用并扩展了源自 802.11n 的空中接口（air interface）概念，包括：更宽的 RF 带宽（提升至 160MHz），更多的 MIMO 空间流（spatial streams）（增加到 8），多用户的 MIMO，以及更高阶的调制（modulation）（达到 256QAM）。

参考答案

（45）C　　（46）C　　（47）D

试题（48）

RAID 系统有不同的级别，如果一个单位的管理系统既有大量数据需要存取，又对数据安全性要求严格，那么此时应采用__（48）__。

（48）A．RAID 0　　B．RAID 1　　C．RAID 5　　D．RAID 0+1

试题（48）分析

本题考查 RAID 的基本功能和应用。

独立硬盘冗余阵列（RAID, Redundant Array of Independent Disks），旧称廉价磁盘冗余阵列（Redundant Array of Inexpensive Disks），简称硬盘阵列。其基本思想就是把多个相对便宜的硬盘组合起来，成为一个硬盘阵列组，使性能达到甚至超过一个价格昂贵、容量巨大的硬盘。根据选择的版本不同，RAID 比单颗硬盘有以下一个或多个方面的好处：增强数据集成度，增强容错功能，增加处理量或容量。另外，磁盘阵列对于电脑来说，看起来就像一个单独的硬盘或逻辑存储单元，分为 RAID-0、RAID-1、RAID-1E、RAID-5、RAID-6、RAID-7、RAID-10、RAID-50、RAID-60。

① RAID0：它将两个以上的磁盘串联起来，成为一个大容量的磁盘。在存放数据时，分段后分散存储在这些磁盘中，因为读写时都可以并行处理，所以在所有的级别中，RAID 0 的速度是最快的。但是 RAID 0 既没有冗余功能，也不具备容错能力，如果一个磁盘（物理）损坏，所有数据都会丢失。

② RAID1：将两组以上的 N 个磁盘相互作镜像，在一些多线程操作系统中能有很好的读取速度，理论上读取速度等于硬盘数量的倍数，另外写入速度有微小的降低。只要一个磁盘正常即可维持运作，可靠性最高。

③ RAID5：这是一种储存性能、数据安全和存储成本兼顾的存储解决方案。它使用的是 Disk Striping（硬盘分区）技术。RAID 5 至少需要三颗硬盘，RAID 5 不是对存储的

数据进行备份，而是把数据和相对应的奇偶校验信息存储到组成 RAID5 的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当 RAID5 的一个磁盘数据发生损坏后，可以利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据。RAID 5 可以理解为是 RAID 0 和 RAID 1 的折衷方案。

④ RAID0+1：这是 RAID 0 和 RAID 1 的组合形式，也称为 RAID 01。该方案是存储性能和数据安全兼顾的方案。它在提供与 RAID 1 一样的数据安全保障的同时，也提供了与 RAID 0 近似的存储性能。

参考答案

（48）D

试题（49）

采用 ECC 内存技术，一个 8 位的数据产生的 ECC 码要占用 5 位的空间，一个 32 位的数据产生的 ECC 码要占用__（49）__位的空间。

（49）A. 5　　B. 7　　C. 20　　D. 32

试题（49）分析

本题考查服务器技术的相关概念。

ECC（Error Checking and Correcting，错误检查和纠正）不是一种内存类型，只是一种内存技术。ECC 纠错技术也需要额外的空间来储存校正码，但其占用的位数跟数据的长度并非成线性关系。

ECC 码将信息进行 8 比特位的编码，采用这种方式可以恢复 1 比特的错误。每一次数据写入内存的时候，ECC 码使用一种特殊的算法对数据进行计算，其结果称为校验位（Check Bits）。然后将所有校验位加在一起的和是“校验和”（checksum），校验和与数据一起存放。当这些数据从内存中读出时，采用同一算法再次计算校验和，并和前面的计算结果相比较，如果结果相同，说明数据是正确的，反之说明有错误，ECC 可以从逻辑上分离错误并通知系统。当只出现单比特错误的时候，ECC 可以把错误改正过来不影响系统运行。

一个 8 位的数据产生的 ECC 码要占用 5 位的空间， 16 位数据需占用 6 位；而 32 位的数据则只需再在原来基础增加一位，即 7 位的 ECC 码即可，以此类推。

参考答案

（49）B

试题（50）

在微软 64 位 Windows Server 2008 中集成的服务器虚拟化软件是__（50）__。

（50）A. ESX Server　　B. Hyper-V　　C. XenServer　　D. vserver

试题（50）分析

本题考查服务器技术的相关概念。

虚拟化打破了底层设备、操作系统、应用程序，以及用户界面之间牢固绑定的纽带，

彼此之间不再需要紧密耦合，从而可以变成可以按需递交的服务。最终可以实现这样的目标：在任何时间、任何地方，任何用户可以访问任何应用程序，都可以获得任何所需的用户体验。

选项中 ESX Server 是由 VMware 开发的 VMware ESX Server 服务器，该服务器在通用环境下分区和整合系统的虚拟主机软件。

Hyper-V 是由 Windws Server 2008 中集成的服务器虚拟化软件，其采用微内核架构，兼顾了安全性和性能的要求。

XenServer 是思杰基于 Linux 的虚拟化服务器，是一种全面而易于管理的服务器虚拟化平台，基于 Xen Hypervisor 程序之上。

Vserver 是服务器虚拟化软件，可在一台物理服务器上创建多个虚拟机，每个虚拟机相互独立，相互隔离，且像物理机一样拥有自己的 CPU、内存、磁盘和网卡等资源，从而实现物理服务器的虚拟化，同时运行多个业务系统而互不影响。

参考答案

（50）B

试题（51）

跟网络规划与设计生命周期类似，网络故障的排除也有一定的顺序。在定位故障之后，合理的故障排除步骤为<u>（51）</u>。

（51）A．搜集故障信息，分析故障原因，制定排除计划，实施排除行为，观察效果
B．观察效果，分析故障原因，搜集故障信息，制订排除计划，实施排除行为
C．分析故障原因，观察效果，搜集故障信息，实施排除行为，制订排除计划
D．搜集故障信息，观察效果，分析故障原因，制订排除计划，实施排除行为

试题（51）分析

本题考查故障排除流程。

网络故障的排除先需定位故障，分析故障原因，然后制定排除计划，实施排除行为，观察效果。

参考答案

（51）A

试题（52）

组织和协调是生命周期中保障各个环节顺利实施并进行进度控制的必要手段，其主要实施方式为<u>（52）</u>。

（52）A．技术审查 B．会议 C．激励 D．验收

试题（52）分析

本题考查生命周期相关阶段任务。

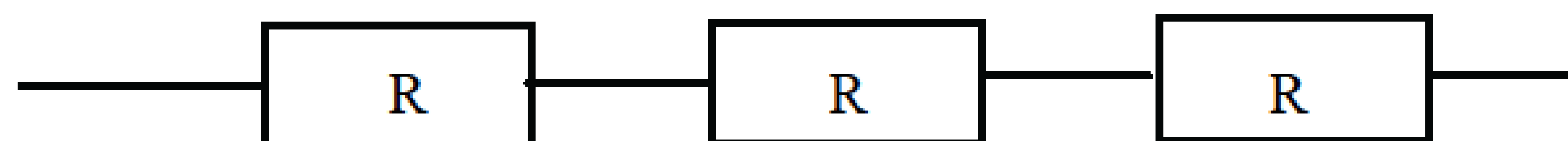
组织和协调是进度控制的必要手段，通常采用会议形式进行。

参考答案

（52）B

试题（53）

三个可靠度 R 均为 0.9 的部件串联构成一个系统，如下图所示：



则该系统的可靠度为＿（53）＿。

（53）A．0.810　　B．0.729　　C．0.900　　D．0.992

试题（53）分析

本题考查系统可靠度。

由于串联，故可靠度为 0.9*0.9*0.9＝0.729。

参考答案

（53）B

试题（54）

在下列业务类型中，上行数据流量远大于下行数据流量的是＿（54）＿。

（54）A．P2P　　B．网页浏览　　C．即时通信　　D．网络管理

试题（54）分析

本题考查网络应用的基本知识。

P2P 是 Peer-to-Peer 的缩写。P2P 网中所有参与系统的结点处于完全对等的地位，即在覆盖网络中的每一个结点都同时扮演着服务器和客户端两种角色，每个在接受来自其他结点的服务同时，也向其他结点提供服务。因此，这类网络业务，上行数据流了与下行数据流量基本相同。

网页浏览是目前互联网上应用最为广泛的一种服务，该服务的运行是基于 B/S 结构的，即用户通过浏览器向服务器发送一个网页请求，服务器再将该网页数据返回给用户，这种模式下，下行数据流量将远大于上行数据流量。

即时通信是使用相应的即时通信软件实现用户之间实时通信和交流的一种互联网服务。在该服务中，用户在发送数据的同时也在接收数据，双向数据流量基本相同。

网络管理是网络管理员通过 SNMP 协议对网络设备发送大量管理命令和管理信息，而对于命令的接收者并无或者极少的信息反馈给管理端，在这种业务中，上行流量远远大于下行数据流量。

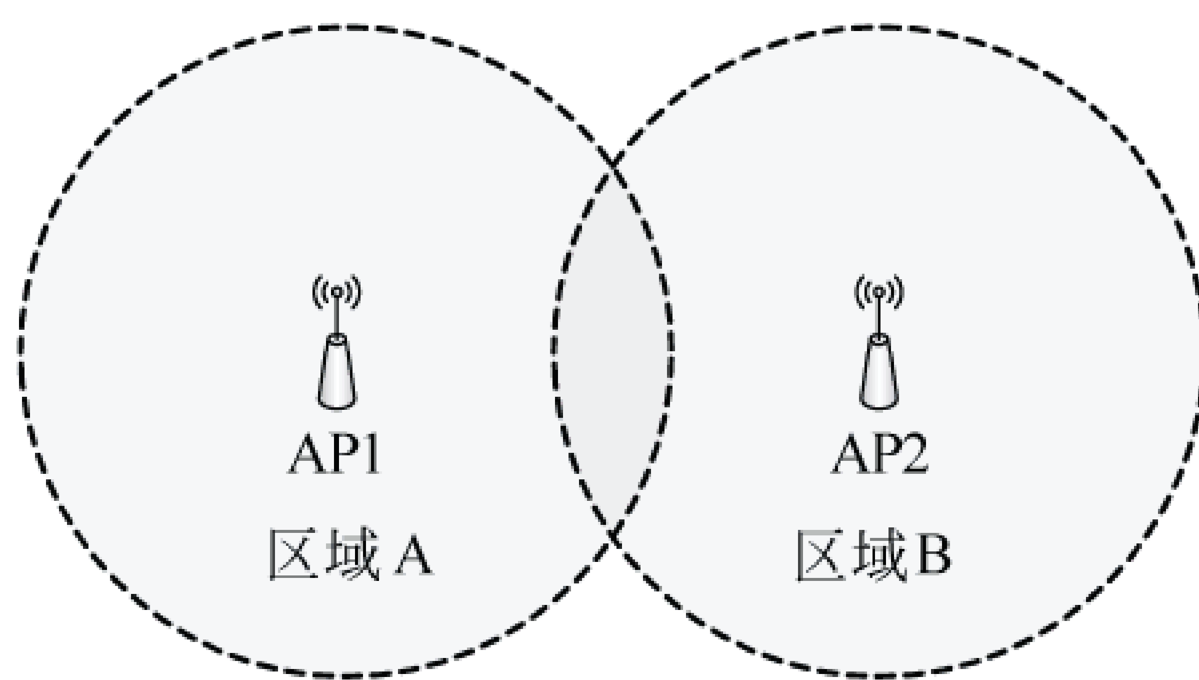
参考答案

（54）D

试题（55）

企业无线网络规划的拓扑图如下所示，使用无线协议是 802.11b/g/n，根据 IEEE 规

定，如果 AP1 使用 1 号信道，AP2 可使用的信道有 2 个，是 （55） 。



（55）A. 2 和 3　　B. 11 和 12　　C. 6 和 11　　D. 7 和 12

试题（55）分析

本题考查无线网络的基本知识。

2.4GHz 无线网络信道划分是按照每 5MHz 一个信道划分，每个信道 22MHz，将 2.4GHz 频段划分出 13 个信道，而这 13 个信道中有相互覆盖和相互重叠的情况，为了无线网络能够互不干扰的工作，在 13 个信道中，只有 3 个信道可用，1、6、11 号信道。

参考答案

（55）C

试题（56）

目前大部分光缆工程测试都采用 OTDR（光时域反射计）来进行光纤衰减的测试，OTDR 通过测试来自光纤的背向散射光来进行测试。这种情况下采用 （56） 方法比较合适。

（56）A. 双向测试　　B. 单向测试　　C. 环形测试　　D. 水平测试

试题（56）分析

本题考查利用 OTDR（光时域反射计）进行光缆测试的方法。目前大部分工程测试都采用 OTDR（光时域反射计）来进行光纤衰减的测试的，而 OTDR 是通过测试来自光纤的背向散射光实现测试的。这样，因为两个方向的散射光往往是不同的，从而导致两个方向测试的结果不同。严格地说，两个方向测试结果都与实际衰减值不同。将两个方向的测试结果取代数和，再除 2（这个方法也适合接头衰减的测试）的结果比较接近实际指标，因此就规定双向测试方法。

参考答案

（56）A

试题（57）

以下关于网络规划需求分析的描述中，错误的是 （57） 。

（57）A. 对于一个新建的网络，网络工程的需求分析不应与软件需求分析同步进行

B. 在业务需求收集环节，主要需要与决策者和信息提供者进行沟通

C. 确定网络预算投资时，需将一次性投资和周期性投资均考虑在内

D．对于普通用户的调查，最好使用设计好的问卷形式进行

试题（57）分析

本题考查网络规划需求分析的基本知识。

在整个网络开发过程中，业务需求调查是理解业务本质的关键，应尽量保证设计的网络能够满足业务的需求，在业务需求收集和调查环节，设计人员须同企业或者部门的领导者进行充分的沟通，已确定网络建设各个方面的需求和问题。

一般在进行网络工程的需求分析时，同时将软件需求分析同步进行，因为网络工程的实施和包括对于网络系统中所使用的软件的安装和调试等环节。

网络预算一般分为一次性投资预算和周期性投资预算，一般来说年度发生的周期性投资预算和一次性投资预算之间的比例为 10%～15%是比较合理的。一次性投资预算主要用于网络的初始建设，包括设备采购、购买软件、维护和测试系统，培训工作人员以及设计和安装系统的费用等；应根据一次性投资预算，对设备、软件进行选型，对培训工作量进行限定，确保网络初始建设的可行性。周期性投资预算主要用于后期的运营维护，包括人员消耗、设备维护消耗、软件系统升级消耗、材料消耗、信息费用、线路租用费用等多个方面；同时，对客户单位的网络工作人员的能力进行分析，考察他们的工作能力和专业知识是否能够胜任以后的工作，并提出相应的建议，是评判周期性投资预算是否能够满足运营需要的关键之一。

对于普通用户的调查过程一般采用问卷调查的方式进行，这种方式能够更好地提高调查的效率和调查结果的可用性。

参考答案

（57）A

试题（58）

在局域网中，划分广播域的边界是<u>（58）</u>。

（58）A．HUB　　B．Modem　　C．VLAN　　D．交换机

试题（58）分析

本题考查网络设备的基本知识。

HUB 也叫集线器，是一种总线型的网络连接设备，工作于 OSI 模型的物理层，使用集线器所连接的网络拓扑为总线型网络，它是一个广播域，同时也是冲突域。

Modem 是调制解调器，主要为实现在传统模拟线路上传输数字信号的一种设备。

VLAN 是一种通过逻辑地在交换机上根据一定的规则分隔广播数据包的方式，通过为进入交换机的数据帧标记不同的 vlan tag，只有带有与接口相同的 vlan tag 的数据帧才能够被转发和通信。

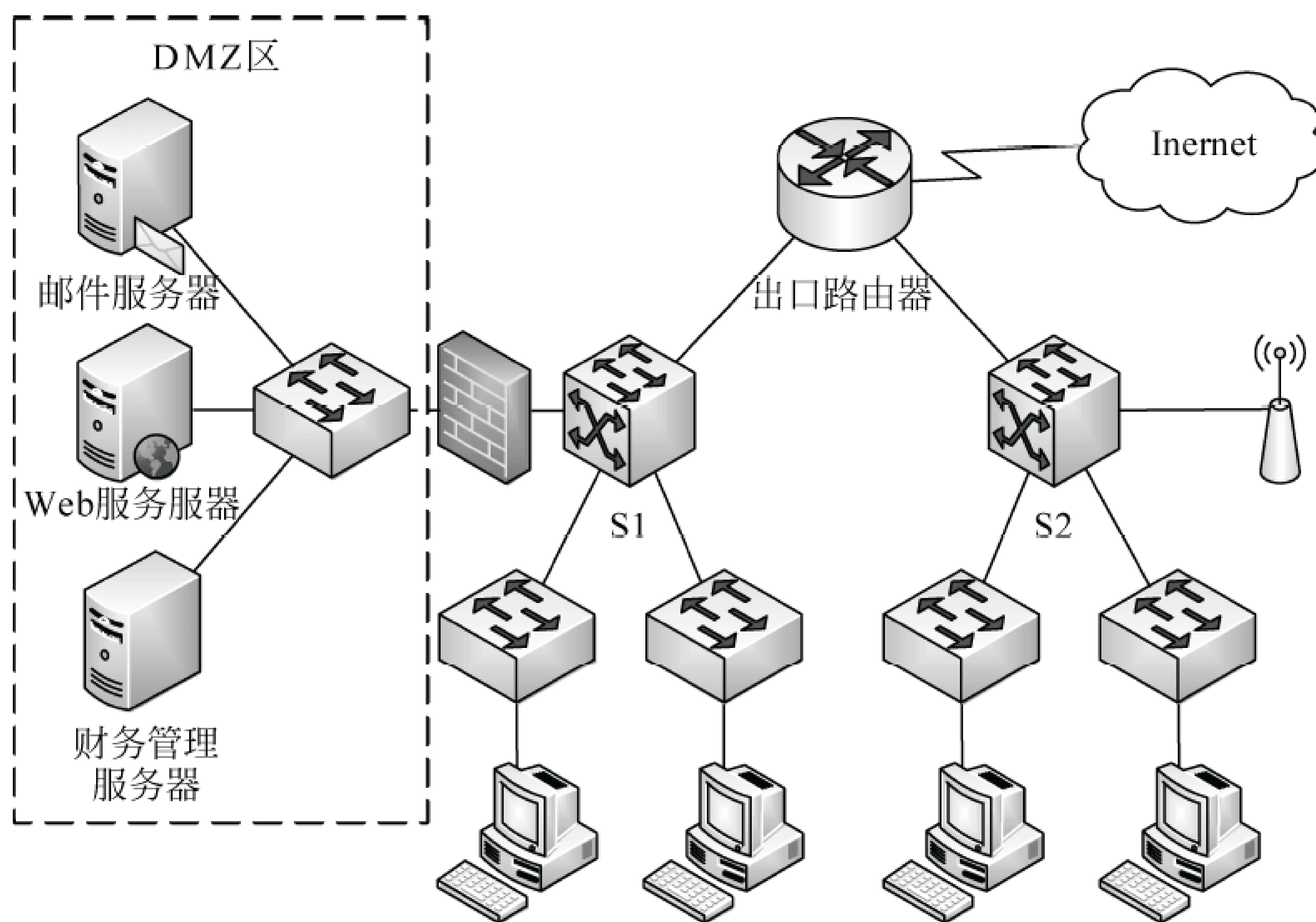
交换机在默认情况下，所有的接口均处于同一个广播域中，因此它不具备划分广播域边界的功能。

参考答案

（58）C

试题（59）

工程师为某公司设计了如下网络方案。



下面关于该网络结构设计的叙述中，正确的是＿（59）＿。

（59）A．该网络采用三层结构设计，扩展性强

B．S1、S2 两台交换机为用户提供向上的冗余连接，可靠性强

C．接入层交换机没有向上的冗余连接，可靠性较差

D．出口采用单运营商连接，带宽不够

试题（59）分析

本题考查网络设计部署的基本知识。

根据图示的拓扑链接可见，该网络规划采用的是两层结构的扁平化设计方式，而两台核心层交换机 S1、S2 之间并未提供冗余连接，这样的连接方式，会造成很严重的单点故障，因此不能为整个网络提供较高的可靠性。Internet 接入采用单运营商接入的方式，并不能够导致带宽不够的问题，而接入层向核心层并未提供冗余连接，网络的可靠性较差。

参考答案

（59）C

试题（60）

下面关于防火墙部分连接的叙述中，错误的是＿（60）＿。

（60）A．防火墙应与出口路由器连接

B．Web 服务器连接位置恰当合理

C．邮件服务器连接位置恰当合理

D．财务管理服务器连接位置恰当合理

试题（60）分析

本题考查网络服务器部署的基本知识。

网络中的防火墙位置可放置于接入互联网的路由器之前，也可将其放置于网络的核心层，以提高内部网络用户的使用体验，在防火墙的 DMZ 区中，所放置的可以是为内部网络用户或者外部网络用户提供服务的各类服务器，而财务管理服务器不属于公共服务器，应放置于专用网络中。

参考答案

（60）D

试题（61）

下面关于用户访问部分的叙述中，正确的是＿（61）＿。

（61）A．无线接入点与 S2 相连，可提高 WLAN 用户的访问速率

B．有线用户以相同的代价访问 Internet 和服务器，设计恰当合理

C．可增加接入层交换机向上的冗余连接，提高有线用户访问的可靠性

D．无线接入点应放置于接入层，以提高整个网络的安全性

试题（61）分析

本题考查接入层网络部署的基本知识。

网络接入层的作用是为用户提供接入到网络的接口，无线网络接入点为无线用户提供网络的接入，一般的部署方式是将无线网络接入点放置于网络接入层设备，题（59）的图的设计中，将无线接入点与核心层设备 S2 相连是不合理的。由于核心层设备为采用冗余连接，因此两端的用户在访问内部服务器时的代价是不同的，同时，即使在接入层添加到核心层的冗余连接，也并不能提高有线网络用户访问内部网络的可靠性，因此该项设计不恰当。

参考答案

（61）D

试题（62）

下列对于网络测试的叙述中，正确的是＿（62）＿。

（62）A．对于网络连通性测试，测试路径无需覆盖测试抽样中的所有子网和 VLAN

B．对于链路传输速率的测试，需测试所有链路

C．端到端链路无需进行网络吞吐量的测试

D．对于网络系统延时的测试，应对测试抽样进行多次测试后取平均值，双向延时应≤1 ms

试题（62）分析

本题考查网络测试的基本知识。

对新建网络进行测试时，无需对链路传输速率、端到端测试和所有子网和 VLAN 进行测试，一般采取抽样测试的方式进行，测试需对所有抽样进行测试，以提高测试的准确性；对于端到端链路测试中，吞吐量的测试是其中一项非常重要的测试项目。

参考答案

（62）D

试题（63）

下列地址中，＿（63）＿是 MAC 组播地址。

（63）A．0x0000.5E2F.FFFF　　B．0x0100.5E4F.FFFF

C．0x0200.5E6F.FFFF　　D．0x0300.5E8F.FFFF

试题（63）分析

本题考查网络地址的基本知识。

MAC（Media Access Control）地址，或称为 MAC 地址、硬件地址，用来定义网络设备的位置。采用十六进制数表示，共六个字节（48 位）。其中，前三个字节是由 IEEE 的注册管理机构 RA 负责给不同厂家分配的代码（高位 24 位），也称为“编制上唯一的标识符”（Organizationally Unique Identifier），后三个字节（低位 24 位）由各厂家自行指派给生产的适配器接口，称为扩展标识符（唯一性）。一个地址块可以生成 224 个不同的地址。

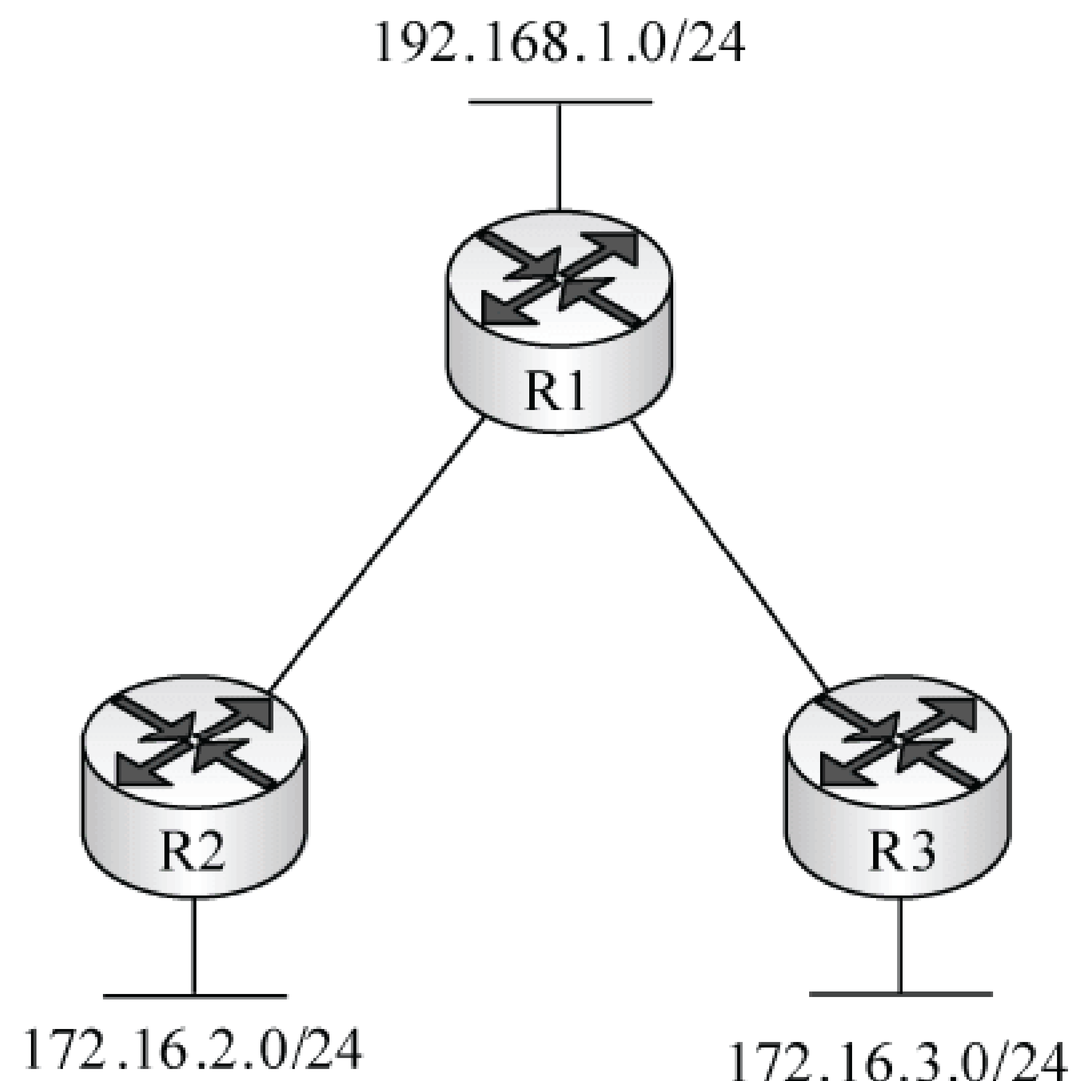
MAC 地址中有一部分保留地址用于组播，范围是 0100.5E00.0000---0100.5E07.FFFF。

参考答案

（63）B

试题（64）

某网络拓扑图如下所示，三台路由器上均运行 RIPv1 协议，路由协议配置完成后，测试发现从 R1 ping R2 或者 R3 的局域网，均有 50%的丢包，出现该故障的原因可能是＿（64）＿。



（64）A．R1 与 R2、R3 的物理链路连接不稳定

B．R1 未能完整的学习到 R2 和 R3 的局域网路由

C．管理员手工的对 R2 和 R3 进行了路由汇总

D．RIP 协议版本配置错误，RIPv1 不支持不连续子网

试题（64）分析

本题考查网络路由协议的基本知识。

三台路由器运行 RIPv1 协议，从 R1 ping R2 或者 R3 的局域网，出现均有 50%的丢包现象，RIPv1 不支持不连续的子网，因此，在 R1 上针对 R2 和 R3 局域网的 172.16.2.0/24 和 172.16.3.0/24 路由进行了路由汇总，统一汇总成 172.16.0.0/16 路由，因此，当从 R1 ping R2 或者 R3 时，路由器认为从 R1 与 R2 和 R3 相连的接口均可到达，实现了不恰当的负载均衡。

参考答案

（64）D

试题（65）

使用长度 1518 字节的帧测试网络吞吐量时，1000M 以太网抽样测试平均值是__（65）__时，该网络设计是合理的。

（65）A．99%　　B．80%　　C．60%　　D．40%

试题（65）分析

本题考查网络测试的基本知识。

吞吐率是指空载网络在没有丢包的情况下，被测网络链路所能达到的最大数据包转发速率。吞吐率测试需按照不同的帧长度（包括 64、128、256、512、1024、1280、1518 字节）分别进行测量。系统在帧长度为 1518 字节测试 1000M 以太网时，测试平均值应为 99%时，网络设计达到要求。

参考答案

（65）A

试题（66）

某企业内部两栋楼之间距离为 350 米，使用 62.5/125μm 多模光纤连接。100Base-FX 连接一切正常，但是该企业将网络升级为 1000Base-SX 后，两栋楼之间的交换机无法连接。经测试，网络链路完全正常。解决此问题的方案是__（66）__。

（66）A．把两栋楼之间的交换机模块更换为单模模块

B．把两栋楼之间的交换机设备更换为路由器设备

C．把两栋楼之间的多模光纤更换为 50/125μm 多模光纤

D．把两栋楼之间的多模光纤更换为 8/125μm 单模光纤

试题（66）分析

本题考查网络故障解决方法。两栋楼距离 350 米，使用多模光纤连接，由 100Base-FX

升级至 1000Base-SX 后无法连通。根据光纤传输知识可知，1000BASE-SX 所使用的光纤有：波长为 850nm，分为 62.5/125 μm 多模光纤、50/125μm 多模光纤。其中使用 62.5/125 μm 多模光纤的最大传输距离为 220m，使用 50/125μm 多模光纤的最大传输距离为 500 米。因此只需要将两栋楼之间的多模光纤更换为 50/125μm 多模光纤即可。

参考答案

（66）C

试题（67）

IANA 在可聚合全球单播地址范围内指定了一个格式前缀来表示 IPv6 的 6to4 地址，该前缀为＿（67）＿。

（67）A．0x1001　　B．0x1002　　C．0x2002　　D．0x2001

试题（67）分析

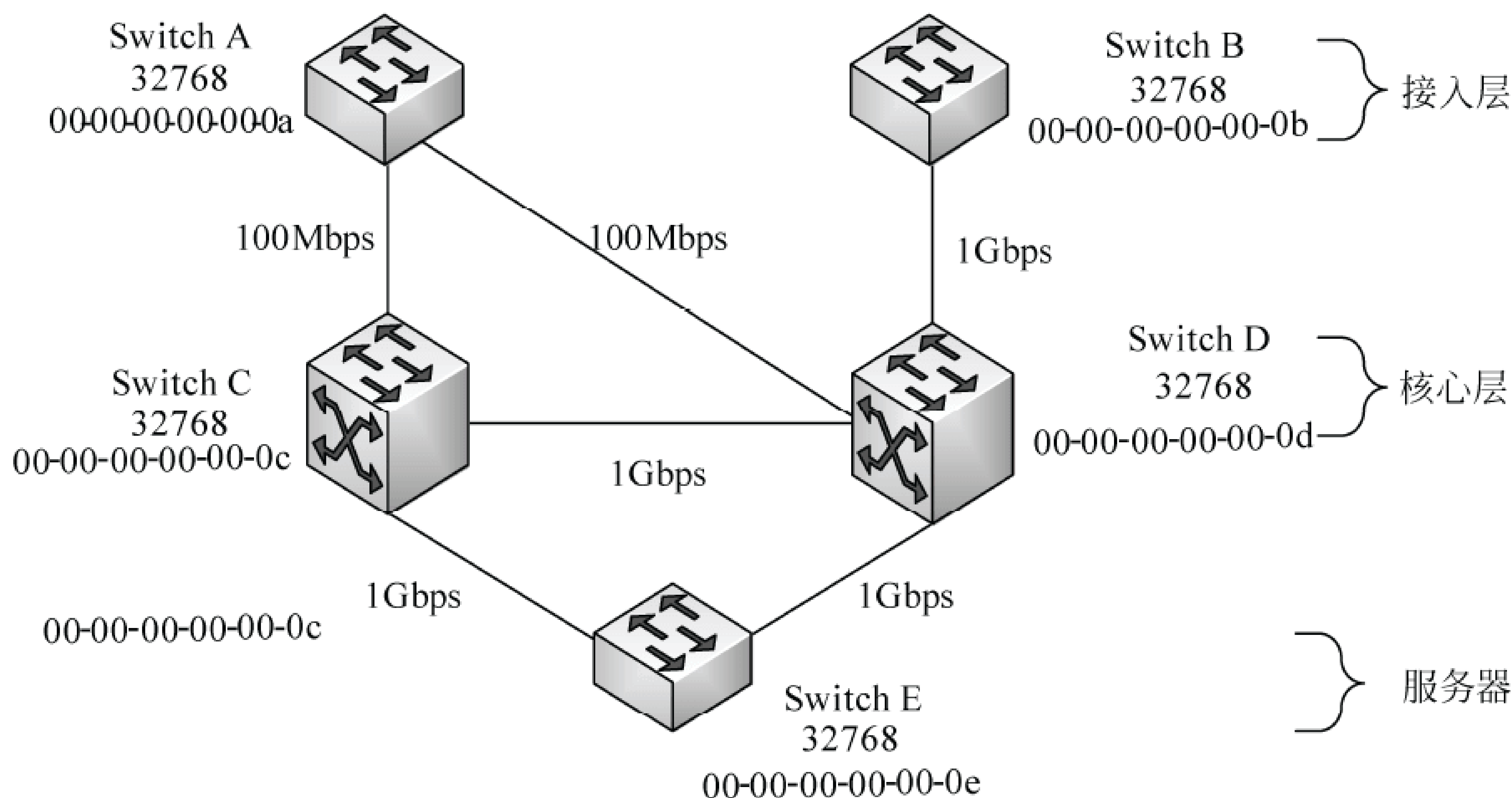
本题考查可聚合全球单播地址的知识。6to4 隧道采用特殊的 IPv6 地址。IANA（因特网编号分配委员会）为 6to4 隧道方式地分配了一个永久性的 IPv6 格式前缀 0x2002，表示成 IPv6 地址前缀格式为 2002::/16。如果一个用户站点拥有至少一个有效的全球唯一的 32 位 IPv4 地址（v4ADDR），那么该用户站点将不需要任何分配申请即可拥有如下的 IPv6 地址前缀 2002v4ADDR)::/48。

参考答案

（67）C

试题（68）～（70）

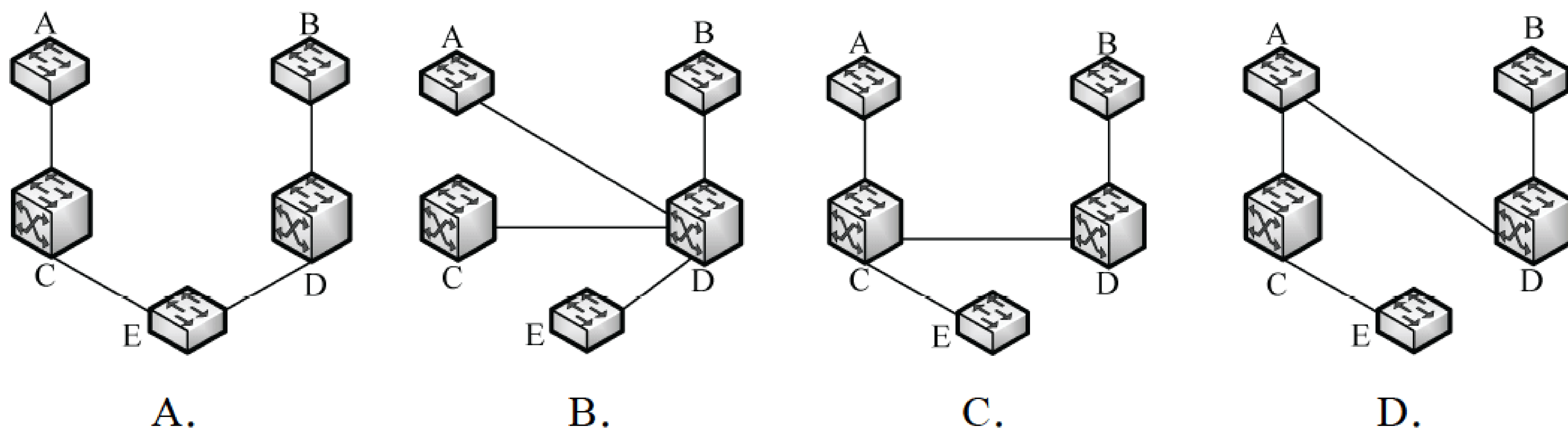
图中所示是一个园区网的一部分，交换机 A 和 B 是两台接入层设备，交换机 C 和 D 组成核心层，交换机 E 将服务器群连接至核心层。如图所示，如果采用默认的 STP 设置和默认的选举过程，其生成树的最终结果为＿（68）＿。



这时交换机 B 上的一台工作站要访问园区网交换机 E 上的服务器其路径为＿（69）＿。

由此可以看出，如果根网桥的选举采用默认配置，下列说法中不正确的是__（70）__。

（68）



（69）A．B—D—E　　B．B—D—C—E

C．B—D—A—C—E　　D．不能抵达

（70）A．最慢的交换机有可能被选为根网桥

B．有可能生成低效的生成树结构

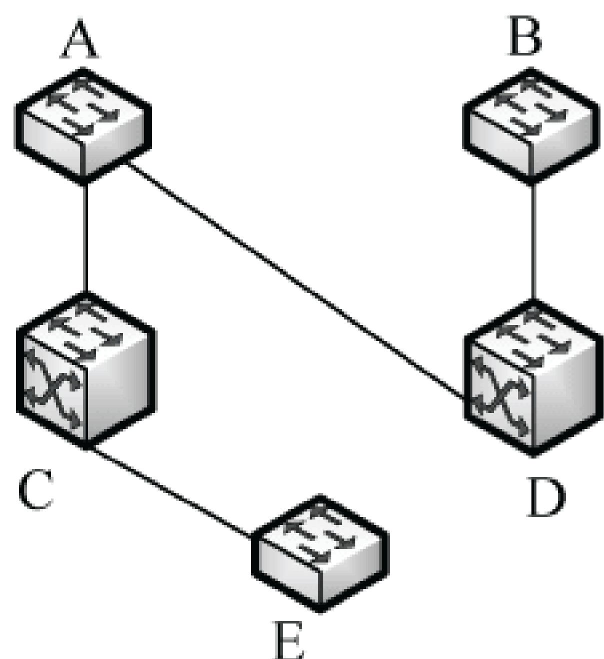
C．只能选择一个根网桥，没有备用根网桥

D．性能最优的交换机将被选为根网桥

试题（68）～（70）分析

本题考查 STP 相关知识。

如图所示，在默认 STP 设置下，接入层交换机 A 将成为根网桥，因为它的 MAC 地址最小，而所有交换机的优先级都一样。这样交换机 A 被选作根后，它就不能使用 1Gbps 的链路，它只有两条 100Mbps 的链路。根据默认的选举过程，删除处于阻断状态的链路后的网络，从中可以看出生成树的最终结果（如下图所示）。接入交换机 A 是根交换机，在交换机 B 上的工作站必须通过核心层（交换机 D）、接入层（交换机 A）和核心层（交换机 C），才能最后到达交换机 E 上的服务器，显然这种行为是低效的。STP 可以自动地使用默认设置和默认选举过程，但得到的树结构可能与预期的截然不同。



参考答案

（68）D　（69）C　（70）D

试题（71）～（75）

There are two general approaches to attacking a __（71）__ encryption scheme. The first

attack is known as cryptanalysis. Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the __(72)__ or even some sample plaintext-ciphertext pairs. This type of __(73)__ exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised. The second method, known as the __(74)__ -force attack, is to try every possible key on a piece of __(75)__ until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

（71）	A. stream	B. symmetric	C. asymmetric	D. advanced
（72）	A. operation	B. publication	C. plaintext	D. ciphertext
（73）	A. message	B. knowledge	C. algorithm	D. attack
（74）	A. brute	B. perfect	C. attribute	D. research
（75）	A. plaintext	B. ciphertext	C. sample	D. code

参考译文

有两种常用的方法可以攻击对称密钥加密方案。第一种攻击叫做密码分析学。密码分析攻击依赖于算法的特性，也许还要加上某些有关明文的一般性特征的知识，甚至需要某些明文-密文对的样品作为辅助。这种类型的攻击利用了算法的特点，企图推导出特殊的明文或者推导出当前使用的密钥。如果这种攻击成功地导出了密钥，其效果将是灾难性的：所有将来和过去用这个密钥加密的报文都会被突破。第二种方法叫做蛮力攻击，就是用每一种可能的密钥在一段密文上进行试验，直到将其转换为可理解的明文。平均来说，要达到成功需要试验的密钥数量为各种可能的密钥数量的一半。

参考答案

（71）B （72）C （73）D （74）A （75）B

第 20 章 2014 下半年网络规划设计师下午试题 I 分析与解答

试题一（共 25 分）

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

【说明】

某高校拟对学生公寓网络（已知网络主机超过 3000 台）进行改造，该校网络部门在技术方案讨论的过程中，提出了以太网接入、ADSL 接入和 PON 接入三种思路。该部门技术主管在对三种方案的建设成本、网络安全、系统容易维护、宽带综合业务等方面综合考虑后决定采用 GPON 接入方式，并给出了基于 GPON 技术的学生公寓宽带初步设计方案，如图 1-1 所示。

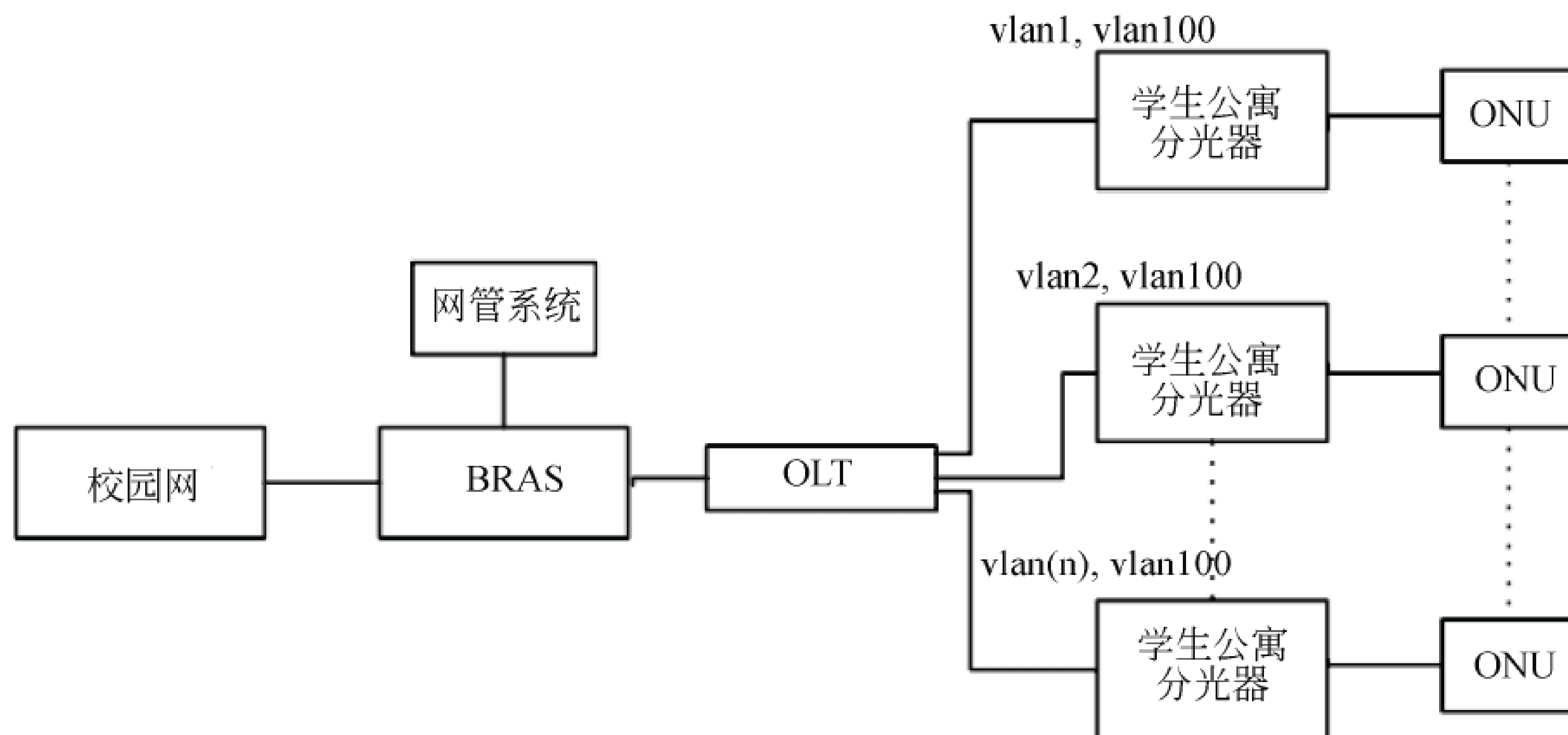


图 1-1

【问题 1】（5 分）

请比较以太网接入、ADSL 接入以及 GPON 接入三种方式的特点，并简要说明选择 GPON 接入方式的理由。

【问题 2】（5 分）

已知网络部门对学生公寓网络分配了一个地址段 59.74.116.0/24。请给出学生公寓网络地址规划与设计方案。

【问题 3】（6 分）

请依据图 1-1 设计方案，并且结合用户上网方式是拨号上网、网络安全控制以及采用带内管理方式管理网络等技术因素。说明 BRAS（Broadband Remote Access Server）和 OLT 设备性能及配置描述。

【问题 4】（5 分）

如果将图 1-1 中 BRAS 设备用路由器（Router）替换，请分析在学生公寓网络规划上可能有哪些变化。

【问题 5】（4 分）

请简要说明 GPON 接入相比 EPON 接入对支持“三网合一”的发展有什么优势。

试题一分析

本题考查网络接入技术以及局域网配置、产品主要性能指标等相关知识即应用。

【问题 1】

无源光纤网络 PON（Passive optical network）又称被动式光纤网络，是光纤通信网络的一种，其特色为不用电源就可以完成信号处理，除了终端设备需要用到电以外，其中间的节点则以精致小巧的光纤元件构成。PON 系统结构主要由中心局的光线路终端（OLT）、包含无源光器件的光分配网（ODN）、用户端的光网络单元/光网络终端（ONU/ONT，其区别为 ONT 直接位于用户端，而 ONU 与用户之间还有其他网络，如以太网）以及网元管理系统（EMS）组成，通常采用点到多点的树型拓扑结构。在下行方向，IP 数据、语音、视频等多种业务由位于中心局的 OLT，采用广播方式，通过 ODN 中的 1:N 无源光分配器分配到 PON 上的所有 ONU 单元。在上行方向，来自各个 ONU 的多种业务信息互不干扰地通过 ODN 中的 1:N 无源光合路器耦合到同一根光纤，最终送到位于局端 OLT 接收端。

【问题 2】

网络地址转换（NAT，Network Address Translation）属接入广域网（WAN）技术，是一种将私有（保留）地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。NAT 不仅可以解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

虚拟局域网（Virtual Local Area Network 或简写 VLAN，V-LAN）是一种建构于局域网交换技术（LAN Switch）的网络管理的技术，网管人员可以借此通过控制交换机有效分派出入局域网的分组到正确的出入端口，达到对不同实体局域网中的设备进行逻辑分群（Grouping）管理，并降低局域网内大量数据流通时，因无用分组过多导致拥塞的问题，以及提升局域网的信息安全保障。

【问题 3】

公寓网络的宽带认证通过 BRAS 实现，从图 1-1 网络拓扑分析，选用集成 PPPoE、DHCP、NAT、防火墙的高性能 BRAS,该 BRAS 上进行 PPPoE 的配置，为每个用户设置账号和密码；启用 DHCP 服务，配置内网地址池；进行 NAT 配置，实现内外网地址转换；进行防火墙规则配置。

OLT 可以选用具有三层交换功能的机架式、大容量、全光接入的产品，单框用户数 128 口，可以满足公寓网络的需求。对于网络系统的管理采用带内方式管理，即网管信

息与业务信息共用同一通道，网管单独用 1 个 VLAN，设为 VLAN100，每个业务端口均要透传 VLAN100。

【问题 4】

1. 网络边界出现变化，学生公寓网络可作为校园网的一个子网成为校园网的一个组成部分。

2. IP 地址分配、用户认证与校园网统一，NAT、认证等功能由上端设备承担。

3. 学生公寓的网络可以有多种上联方式，可以连接校园网、Internet、IPTV、NGN 等。

4. 由于全业务路由器（Service Router）的出现，在网络规划中，路由器与 BRAS 设备在特定场合也可以实现相同的功能。

【问题 5】

GPON 和 EPON 是两种主流的两种 PON 技术，GPON 符合 ITUT 的标准，而 EPON 是 IEEE 指定的标准。从速率上看 GPON 是非对成的下行 2.488G 上行 1.244G，而 EPON 上下行对称 1.25G。从分光比来看，GPON 支持最大 1:128 的分路比，而 EPON 支持 1:32；从承载业务上看 GPON 可以承载 ATM、ETH、TDM 等多种业务而 EPON 仅支持 ETH；在带宽效率、QoS、协议等多个方面，GPON 更具有广泛性。

试题一参考答案

【问题 1】

方　案	特　点
以太网接入	传统局域网采用的组网方式、成本低、多种介质
ADSL 接入	通过电话线就可实现高速网络接入
GPON 接入	成本低、维护简单、高带宽、抗干扰

理由：GPON 是由局端设备 OLT 与多个用户端设备 ONU 之间通过无源光分配网 ODN 连接的光接入网络。“无源”的特性使得成本低、维护简单，可提供千兆级带宽，并且技术成熟、抗干扰，已经逐渐成为当今主流的网络接入方式（三网合一与 FTTH 接入）。

【问题 2】

1. 需要配置一台 DHCP 服务器，实现内网地址的动态分配；

2. 已分配的网段不能满足用户地址分配的需求，需要相应的网络设备启用 NAT 来实现内外网地址的转换；

3. 由于属于一种类型的用户，公寓网络地址分配按选定网段顺次分配即可；

4. 需要对公寓网络进行 VLAN 和子网划分，便于降低冲突域和网络管理；

5. 为了实现子网间的频繁通信，汇聚各子网的设备具有三层交换功能。

【问题 3】

公寓网络的宽带认证通过 BRAS 实现，从图 1-1 网络拓扑分析，选用集成 PPPoE、DHCP、NAT、防火墙的高性能 BRAS，该 BRAS 上进行 PPPoE 的配置，为每个用户设

置账号和密码；启用 DHCP 服务，配置内网地址池；进行 NAT 配置，实现内外网地址转换；进行防火墙规则配置。

OLT 可以选用具有三层交换功能的机架式、大容量、全光接入的产品，单框用户数 128 口，可以满足公寓网络的需求。对于网络系统的管理采用带内方式管理，即网管信息与业务信息共用同一通道，网管单独用 1 个 VLAN，设为 VLAN100，每个业务端口均要透传 VLAN100。

【问题 4】

1. 网络边界出现变化，学生公寓网络可作为校园网的一个子网成为校园网的一个组成部分。

2. IP 地址分配、用户认证与校园网统一，NAT、认证等功能由上端设备承担。

3. 学生公寓的网络可以有多种上联方式，可以连接校园网、Internet、IPTV、NGN 等。

4. 由于全业务路由器（Service Router）的出现，在网络规划中，路由器与 BRAS 设备在特定场合也可以实现相同的功能。

【问题 5】

GPON 接入相比 EPON 接入对支持“三网合一”上的优势：

1. 速率：GPON 支持多种速率等级，可支持上下行不对称速率。EPON 提供的是固定 1.5Gbps 上下行速率。

2. 分路比：GPON 可支持 ClassA、B 和 C，可支持高达 128 的分路比和长达 20km 的传输距离。EPON 通常支持 1∶32 的分路比，10km 的传输距离。

3. 封装：GPON 无论是在传输汇聚层还是在业务适配层的效率都是最高的，其总效率最高，且等效系统成本最低。

试题二（共 25 分）

阅读以下关于某电信运营商网络的叙述，回答问题 1 至问题 4。

【说明】

对电信运营商而言，三网融合在接入控制层面需要考虑怎样引入 IPTV，如何在多业务接入模式下实现综合运营并保障各类业务的服务质量。IPoE 方式提供多业务接入以满足三网融合发展的必要性和可行性，为运营商三网融合业务提供保障。

某电信运营商 IP 城域网拓扑结构图如图 2-1 所示。

【问题 1】（10 分）

电信运营商的网络是一种可管理网络。目前在用户管理方面用得比较多的主流认证技术主要有 PPPoE、基于 Web-Portal 以及 IEEE 802.1x。这三种接入认证技术由于产生的时间，背景各不相同，因此应用的网络环境也不同，各有利弊。下表是这三种认证技术的部分性能比较，请补充完成表 2-1 中的（1）～（10）。

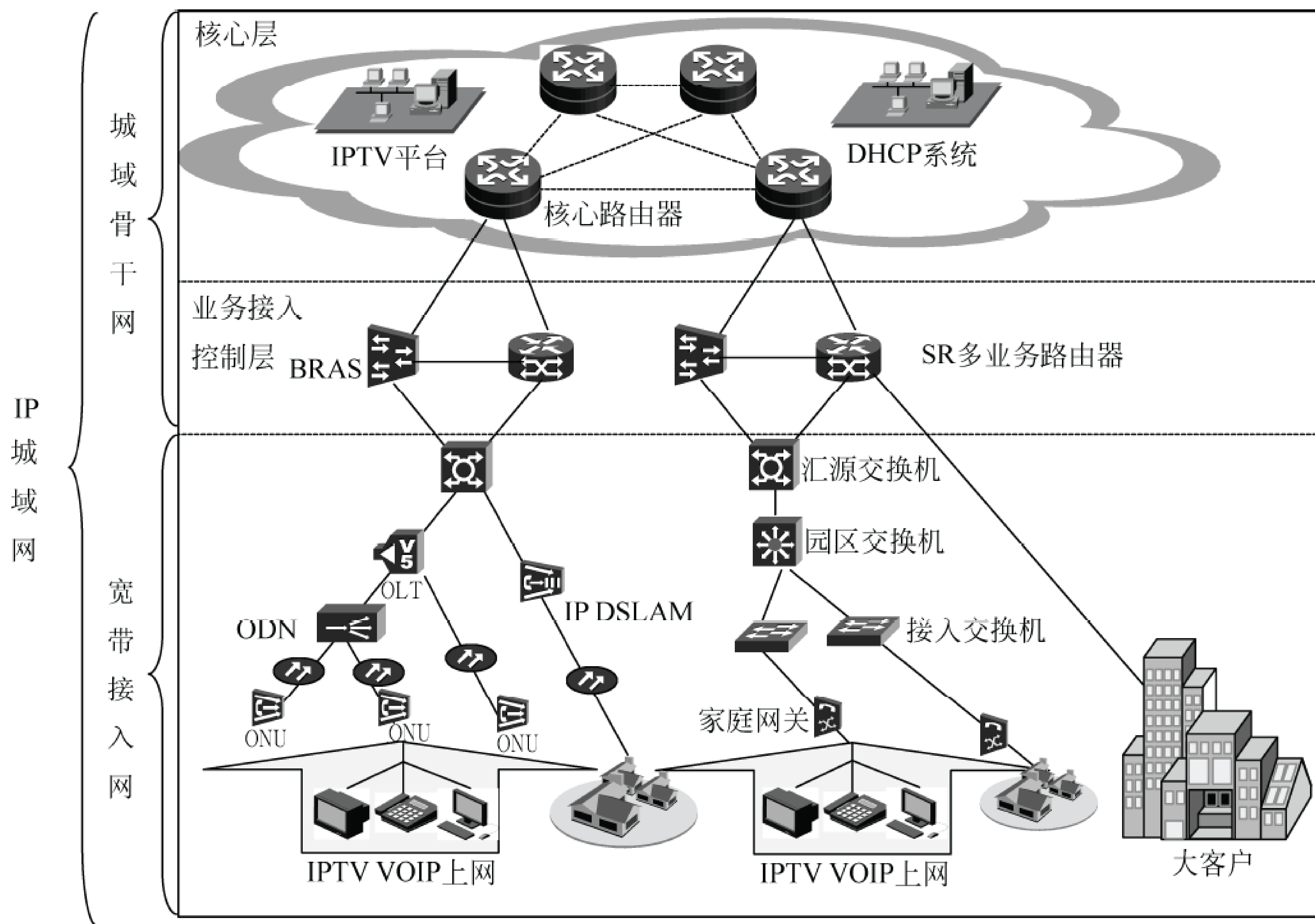


图 2-1

表 2-1　三种认证技术的部分性能指标比较表

基本指标	PPPoE	Web-Portal	802.1x
组网成本	高	高	低
数据报封装开销	(1)	(2)	低
协议运行位置	(3)	(4)	数据链路层
IP 地址分配	认证后分配	(5)	(6)
接入控制	用户	用户	端口
客户端安装	需要	不需要	需要
用户连接性	好	差	好
安全性	高	低	高
业务流与控制流	不分离	(7)	(8)
支持多播业务	(9)	(10)	支持
计费统计精细度	高	低	高

【问题 2】（5 分）

IPoE 和 PPPoE 都是技术较成熟的认证技术，在标准化程度、安全性、精确计费、带宽/端口的控制方面都有相似的优点。

（1）随着 Triple Play“三重播放”业务和以广播 IPTV 为代表的多媒体业务的发展，请简单叙述采用 PPPoE 接入方式会带来的问题。

（2）目前，业界正逐步推动 PPPoE 认证技术向 IPoE 认证技术转换。请简单描述 IPoE 的特点以及大规模商用需解决的关键问题。

【问题 3】（6 分）

IPoE 部署要从运营支撑系统、核心层、业务控制层、接入层分别进行部署。

（1）图 2-1 的 IPoE 部署采用的是多边缘架构进行业务接入区分优化，请对其简单描述一下。

（2）如果对 IPoE 部署采用单边缘架构的部署方案，请对图 2-1 简单修改画出其拓扑结构。

（3）比较多边缘和单边缘两种 IPoE 部署方案的优缺点。

【问题 4】（4 分）

目前电信运营商的用户采用 IPoE 的宽带接入主要认证场景为大客户专线接入认证、IPTV 等。IPoE 和 PPPoE 的交叉场景就是 IPTV，下面就 IPTV 应用 PPPoE 和 IPoE 的场景进行分析。

（1）请在图 2-2 中分别完成 IPTV 使用 PPPoE 和 IPoE 认证方式时多播视频流的流向和流数，并予以简单说明（其中，采用 IPoE 时多播复制点选择在园区交换机和 OLT 上）。

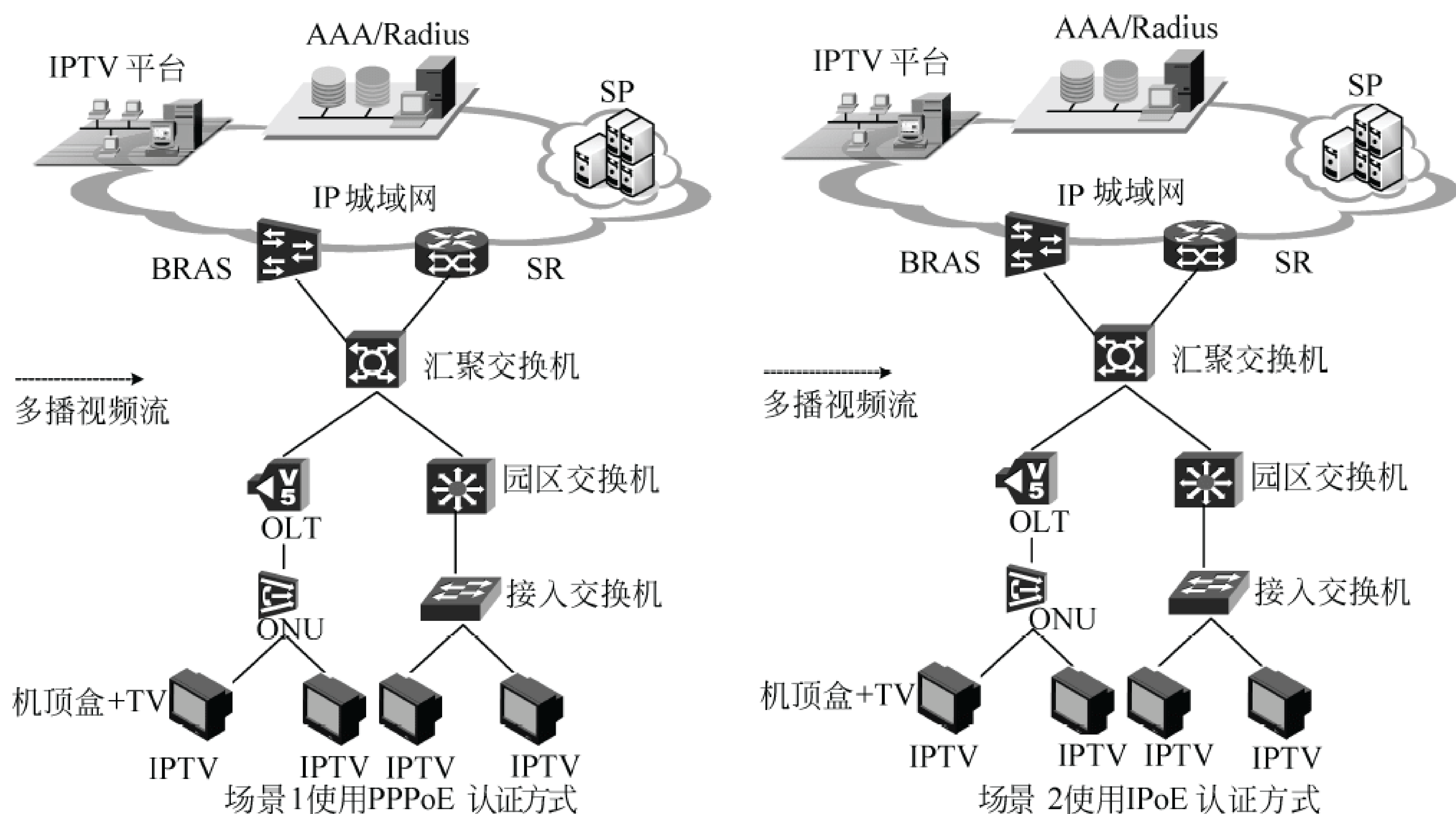


图 2-2

（2）请根据上述比较简要叙述 IPTV 业务发展不同阶段时的认证方式选择。

试题二分析

本题主要考查电信运营商网络中 IPTV 的应用。

【问题 1】

本问题主要考查运营商网络中的接入认证技术。

由于宽带业务的多样化发展趋势，用户接入认证方式作为可运营、可管理的核心，受到包括运营商、制造商、系统集成商的密切关注。当前，电信运营商发展宽带业务主要采用的是 PPPoE 接入方式。随着 IPTV 业务的规模化发展必然进行宽带网组播复制点的下移，接入认证方式将发生重大变革。目前成熟的核心认证技术主要包括 PPPoE 认证、基于 Web-Portal 的认证以及 IEEE 802.1x 认证技术。

PPPoE 继承了 PPP 协议的特点，操作简单且用户较容易接受，能够很好地实现用户计费、在线检测和速率控制等功能。但是，PPPoE 的缺点也同样很明显。PPPoE 所包含的 PPP 包需要被再次封装进以太网报文内才能进行传输，封装效率受到一定影响。由于发现阶段的机制所限，会产生大量的广播包，不但使得网络承受了较大的压力，同时也使得基于组播的业务（如视频会议等）无法开展。除此之外，还需要宽带远程接入服务器 BRAS（Broadband Remote Access Server）的支持，使用这种电信级别的设备成本比较高昂，并且用户的业务数据流和控制认证流都需通过该设备，因此很容易形成网络瓶颈，降低网络性能。

基于 Web-Portal 技术的认证是一种业务类型的认证，由于使用了 Web 页面进行用户名和密码的登入验证，所以省去了安装客户端的麻烦，也避免了系统兼容性的问题。并且，由于承载在应用层之上，无需特别的数据包封装，提高了效率，也减小了网络维护的成本。不过，也正是由于基于 Web-Portal 的认证协议处在 OSI 模型的最高层，所以对设备的要求比较高，建网的成本高。且易用性不高，标准不能统一。IP 地址在用户授权之前就已经分配给用户，不是十分合理。Web 服务器对授权用户和非授权用户来说都是可达的，因此很容易受到恶意攻击，存在安全隐患。同 PPPoE 一样，用户的业务数据流和控制认证流无法区分，造成设备不必要的压力。

IEEE802.1x 就是 IEEE 为了解决基于端口的接入控制而定义的一个标准。作为基于 C/S 的访问控制和认证协议，未经授权的用户或是设备若是未通过 IEEE 802.1x 协议的认证是无法通过接入端口（Access Port）访问网络的。IEEE 802.1x 协议为二层协议不需要到达三层，业务报文直接承载在正常的二层报文上。用户通过认证后实现业务流和认证流分离，不再将数据包进行拆解。IEEE 802.1x 封装效率极高。采用了各端口独立控制处理的方式，因此认证处理容量可以很大，远远高于传统的 BRAS 设备，所有的业务流量和认证系统分开，有效的解决了网络瓶颈问题。与基于七层协议的 Web-Portal 认证相比，能够及时处理异常离线情况和实现基于时间的计费。数据分离的特点使得 IEEE 802.1x 的认证过程变得简单。整个用户认证在二层网络上实现，可以结合 MAC、端口、账户和密码等，具有很高的安全性。

由上述分析可知，这三种接入认证技术应用的网络环境不同，各有利弊。目前三种认证方式都获得了很多成功的应用：PPPoE 现在最主要的用户人群是 ADSL 用户，由电信级别的运营商提供接入服务。而基于 Web-Portal 的认证一般用于旅馆酒店，并多用于无线网络的认证。而 IEEE 802.1x 认证则普遍用于规模较大，接入用户数目庞大的以太网。下表就一些基本的网络数据指标对它们进行了比较。

表 三种认证技术的部分性能指标比较表

基本指标	PPPoE	Web-Portal	802.1x
组网成本	高	高	低
数据报封装开销	高	低	低
协议运行位置	数据链路层	应用层	数据链路层
IP 地址分配	认证后分配	认证前分配	认证后分配
接入控制	用户	用户	端口
客户端安装	需要	不需要	需要
用户连接性	好	差	好
安全性	高	低	高
业务流与控制流	不分离	不分离	分离
支持多播业务	不支持	支持	支持
计费统计精细度	高	低	高

【问题 2】

本问题主要考查在电信运营商的 IPTV 实施中 IPoE 和 PPPoE 各自的技术特点。

（1）对于大量的视频流，只有通过组播方式传送才能最大化地利用带宽，缓解网络瓶颈。而 PPPoE 数据包，给所有数据包都封装 PPP 包头，在 BRAS 与所连接的上万个宽带用户终端之间建立了相同数量的点对点连接。这种方式决定了 BRAS 到所有终端都是唯一的点到点链路，二者之间的任何二层设备对所传送的数据包都没有办法进行组播复制。因此，采用 PPPoE 封装传送广播 IPTV 组播数据流，BRAS 设备会在所有到用户终端的点到点连接上复制组播数据流。这就造成大量数据包在 BRAS 以下的交换机和 EPON 单元上被重复传送，严重浪费 BRAS 下联链路的有限带宽。

BRAS 设备要时刻接受用户拨入请求，与 Radius 服务器合作完成用户的认证工作，同时还要维护大量的 PPPoE 状态信息，对设备的要求是比较高的。IPTV 数据流量大，要求低时延，线速转发，如果进行 PPPoE 数据包封装，在用户量稍大时，BRAS 设备的负载将非常大。采用 PPPoE 技术承载 IPTV 类业务，造成 BRAS 设备处理能力、BRAS 与接入设备之间的带宽两个瓶颈，效率低，扩展性差，基本不能发挥组播技术的优势。

（2）IPoE 认证方式不需要在用户终端上安装任何客户端程序，不需要输入用户名和密码，非常适合新型网络设备，如智能手机，数字电视，PSP（PlayStationPortable，多功能掌机系列，具有游戏、音乐、视频等多项功能）等很难支持内置的 PPPoE 拨号程序的终端应用互联网业务。IPoE 技术的特点：支持用户会话保护，满足运营商对个人宽带业务认证、计费需求；高效的组播传播，适合 IPTV 业务；长接在线，适合语音及视频电话业务；减少多余开销，提高传输效率。

IPoE 技术需要解决的问题：IPoE 认证没有像 PPPoE 认证那样在网络层面提供唯一的点到点的通信机制，运营商在部署 IPoE 认证时，要重点关注安全问题。如：DHCP 溢出攻击和应对策略；ARP 溢出攻击和应对策略；Session 终结管理，根据 DHCP 协议的特性，当 Session 终结后，用户的 IP 地址并不能及时释放并回收。

【问题 3】

本问题主要考查 IPoE 的实际部署。

（1）IPoE 部署要从运营支撑系统、核心层、业务控制层、接入层分别进行部署。具体的运营支撑系统改造方案主要要新建 IPoE 业务的运营支撑系统（DHCP 系统），该系统能够提供用户认证、动态分配地址、动态调整每用户的带宽和 QoS 属性，针对预付费、流量、时长等提供多种计费手段，提供精细化管理和控制。DHCP 系统新增服务器包括认证服务器、DHCP 服务器、Web/Portal 服务器等。在网络部署方案上分为采用多边缘架构进行业务接入区分优化和采用单边缘架构统一业务接入两种方案。

图 2-1 采用的是多边缘架构进行业务接入区分优化方案。其中城域骨干网的设备一般都已支持 IPoE。核心层的设备保持不变，在业务接入控制层根据不同的业务需求进行设备接入区分优化。将宽带接入服务器（BRAS）作为使用 PPPoE 上网业务的边缘控制设备，业务路由器（SR）作为使用 IPoE 的 IPTV、流媒体等关键业务的边缘控制设备，形成多边缘的网络架构。宽带接入网主要将接入层设备改造成支持 IPoE 的设备。接入层设备包括 OLT、EPON、园区交换机和楼道交换机等，需要支持灵活 QinQ、IGMP Snooping、IGMP、IGMP Proxy、 DHCP OPTION 82、 DHCP OPTION 60，并支持对多播频道的控制功能。

（2）采用单边缘架构统一业务接入（如下图所示）。

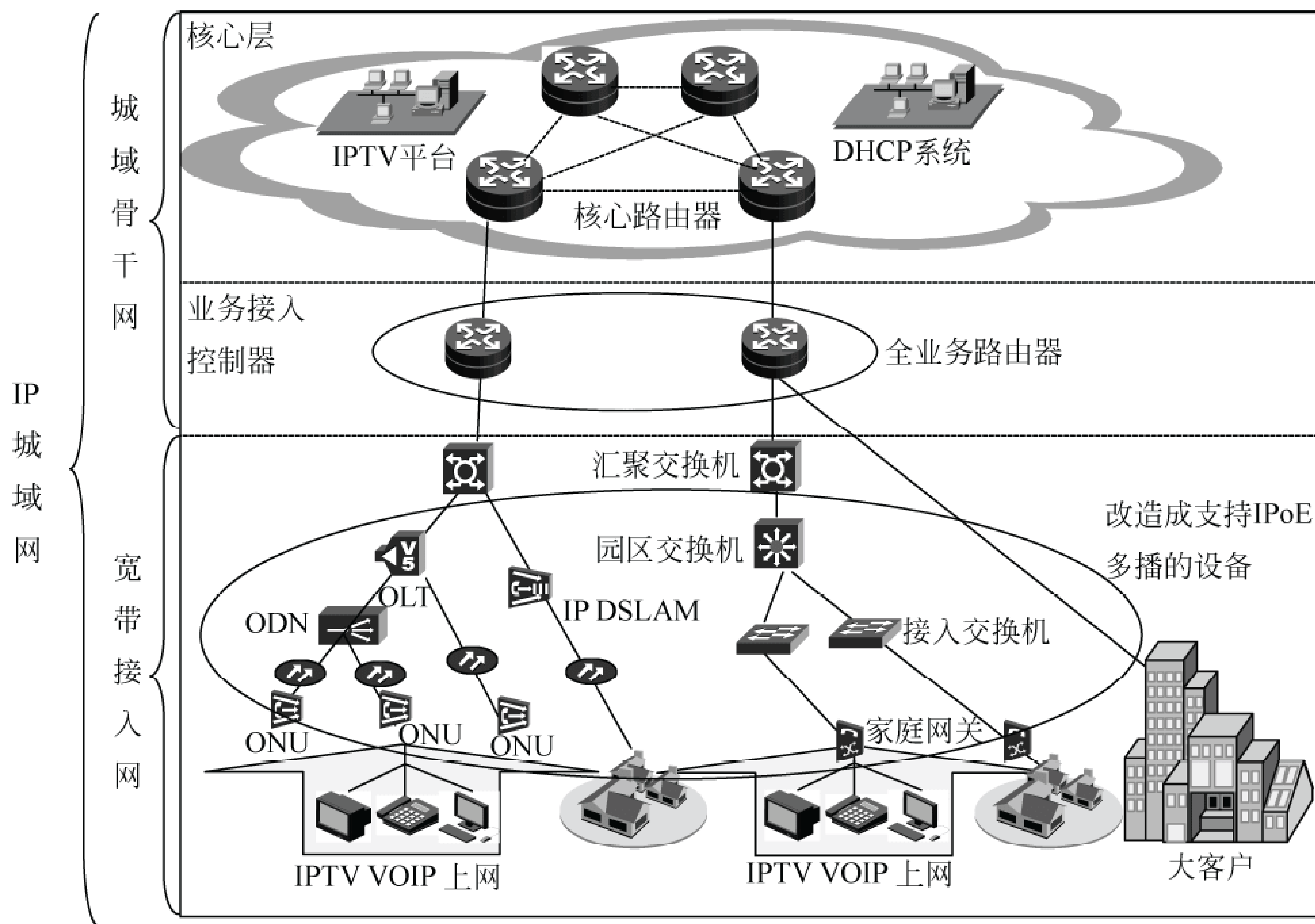


图　采用单边缘架构接入方案图

其中城域骨干网核心层的设备保持不变，在业务接入控制层选择新建全业务路由器，或升级现网 BRAS 为全业务网关来负责业务统一接入，具备 BRAS 和 SR 的功能，并管理 IPoE Session 会话，形成单边缘的网络架构；宽带接入网主要将接入层设备改造成支持 IPoE 的设备。接入层设备包括 OLT、EPON、园区交换机和楼道交换机等，接入层网的改造和采用多边缘架构进行业务接入区分优化的方案一样。

（3）多边缘和单边缘两种 IPoE 部署方案的比较如下表所示。

表　方案比较表

	方案 1（多边缘）	方案 2（单边缘）
优点	实现 IPoE 的部署，有利于 IPTV 等关键业务的扩展； 现网结构保持不变或改动小，投资较小； 上网业务和视频等业务区分接入，可满足不同业务的需求	实现 IPoE 的部署，有利于 IPTV 等关键业务的扩展； 全业务统一接入，便于业务管理； 简化了业务控制层的结构及设备维护； 简化接入层 QoS 的策略部署
缺点	多边缘的网络架构存在多张计费清单，存在同步等问题； 对接入层设备要求高，需对不同业务做分离，接入层 QoS 策略复杂	现网结构改动大，投资大

在一段时间内，IPoE 和 PPPoE 的认证方式会共存并逐步过渡到以 IPoE 为主。IPoE 主要用于 IPTV、NGN、大客户 VPN 等关键业务，为保证 IPTV、NGN、大客户 VPN 等关键业务的承载，运营商往往选择与普通上网业务区分承载层面，因此运营商可根据自身业务的发展情况，在建设、优化 IP 城域网的关键业务平面的同时，选择不同方案统一部署 IPoE。

【问题 4】

本问题主要考查 IPTV 的实际应用场景。

目前电信运营商的用户采用 IPoE 的宽带接入主要认证场景为大客户专线接入认证、IPTV 等。IPoE 和 PPPoE 的交叉场景就是 IPTV，下面就 IPTV 应用 PPPoE 和 IPoE 的不同场景进行分析。

场景 1：使用 PPPoE 认证方式

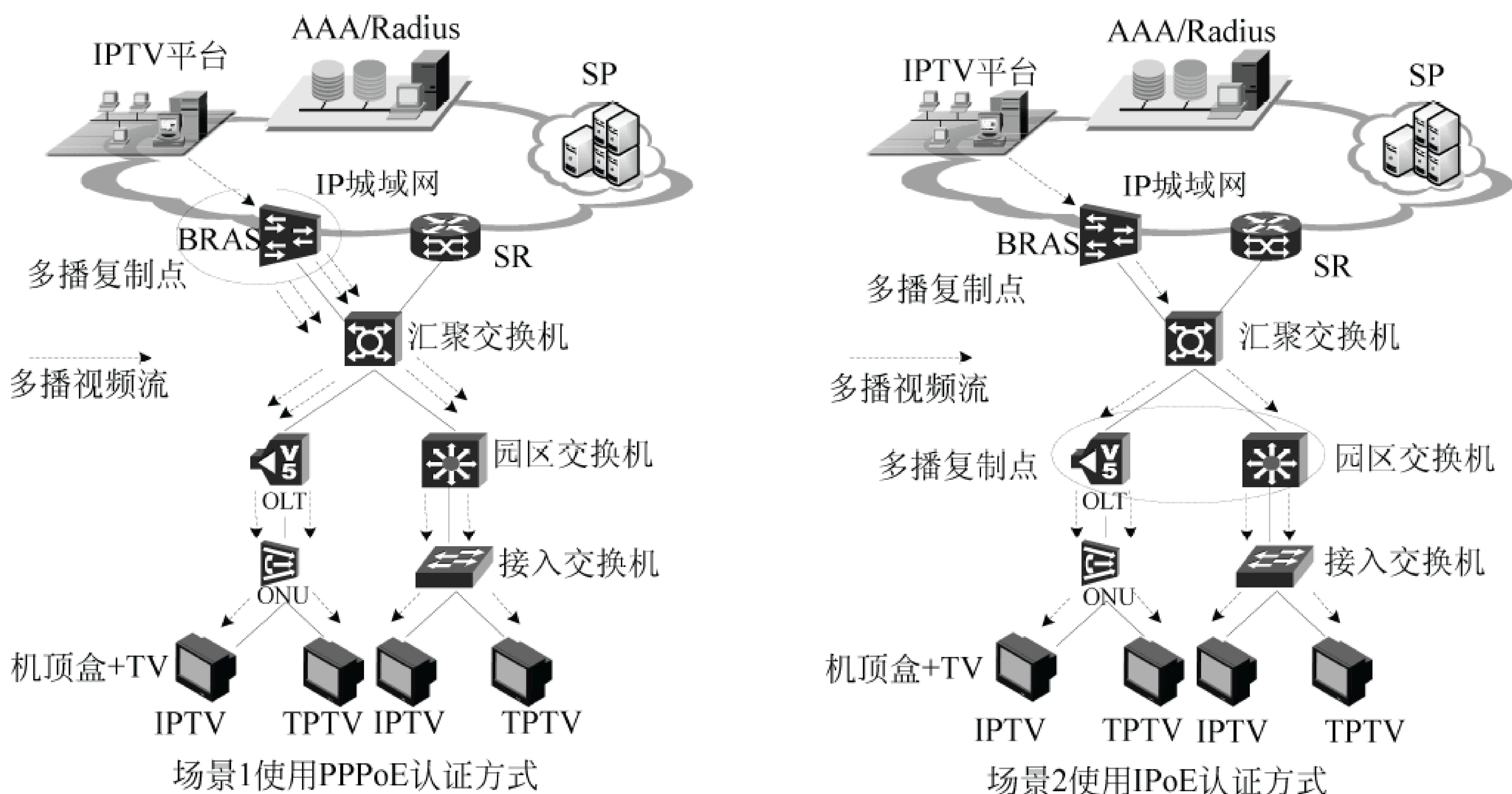
使用 PPPoE 认证，IPTV 的多播复制点只能是 BRAS。如图 2-2 所示，多播复制点为 BRAS，BRAS 面向每个 IPTV 用户都要复制一份数据。这种场景对 BRAS 下行链路（BRAS—汇聚交换机）的带宽，园区交换机、OLT 的上行链路（园区交换机、OLT—汇聚交换机）的带宽及 IP 城域网带宽资源都造成了很大的压力。

场景 2：使用 IPoE 认证方式

使用 IPoE 认证，IPTV 的多播复制点可以灵活选择在 OLT、IP DSLAM、汇聚交换机、园区交换机、接入交换机。如图 2-2 所示，多播复制点为园区交换机和 OLT，由园区交换机、OLT 面向每个 IPTV 用户进行数据复制。这种场景大大节省了 BRAS——园区交换机、OLT 链路的带宽资源，降低了 BRAS 压力。采用 IPoE，播复制点可选择最靠

近用户的设备上，也可采用多级复制、逐级复制进行组播流量的优化。

下图是 IPTV 使用 PPPoE 和 IPoE 认证方式时多播视频流的流向和流数（其中，采用 IPoE 时多播复制点选择在园区交换机和 OLT 上）。



根据上述比较，在 IPTV 发展初期，用户规模比较小时，运营商往往采用 BRAS 接入，通过 PPPoE 协议认证。随着用户规模的逐步扩大，PPPoE 的缺点逐渐显现出来，联带建设成本高，因此，在 IPTV 业务快速发展时，运营商更倾向于采用 IPoE 方式承载 IPTV。

试题二参考答案

【问题 1】

（1）高

（2）低

（3）数据链路层

（4）应用层

（5）认证前分配

（6）认证后分配

（7）不分离

（8）分离

（9）不支持

（10）支持

【问题 2】

（1）

① 严重浪费 BRAS 下联链路的带宽。

② BRAS 设备的负载将非常大。

采用 PPPoE 技术承载 IPTV 类业务，造成 BRAS 设备处理能力、BRAS 与接入设备之间的带宽两个瓶颈，效率低，扩展性差，基本不能发挥组播技术的优势。

（2）

IPoE 技术的特点：支持用户会话保护，满足运营商对个人宽带业务认证、计费需求；高效的组播传播，适合 IPTV 业务；长接在线，适合语音及视频电话业务；减少多余开销，提高传输效率。

IPoE 技术需要解决的问题：IPoE 认证没有像 PPPoE 认证那样在网络层面提供唯一的点到点的通信机制，运营商在部署 IPoE 认证时，要重点关注安全问题。如：DHCP 溢出攻击、ARP 溢出攻击、Session 终结管理等。

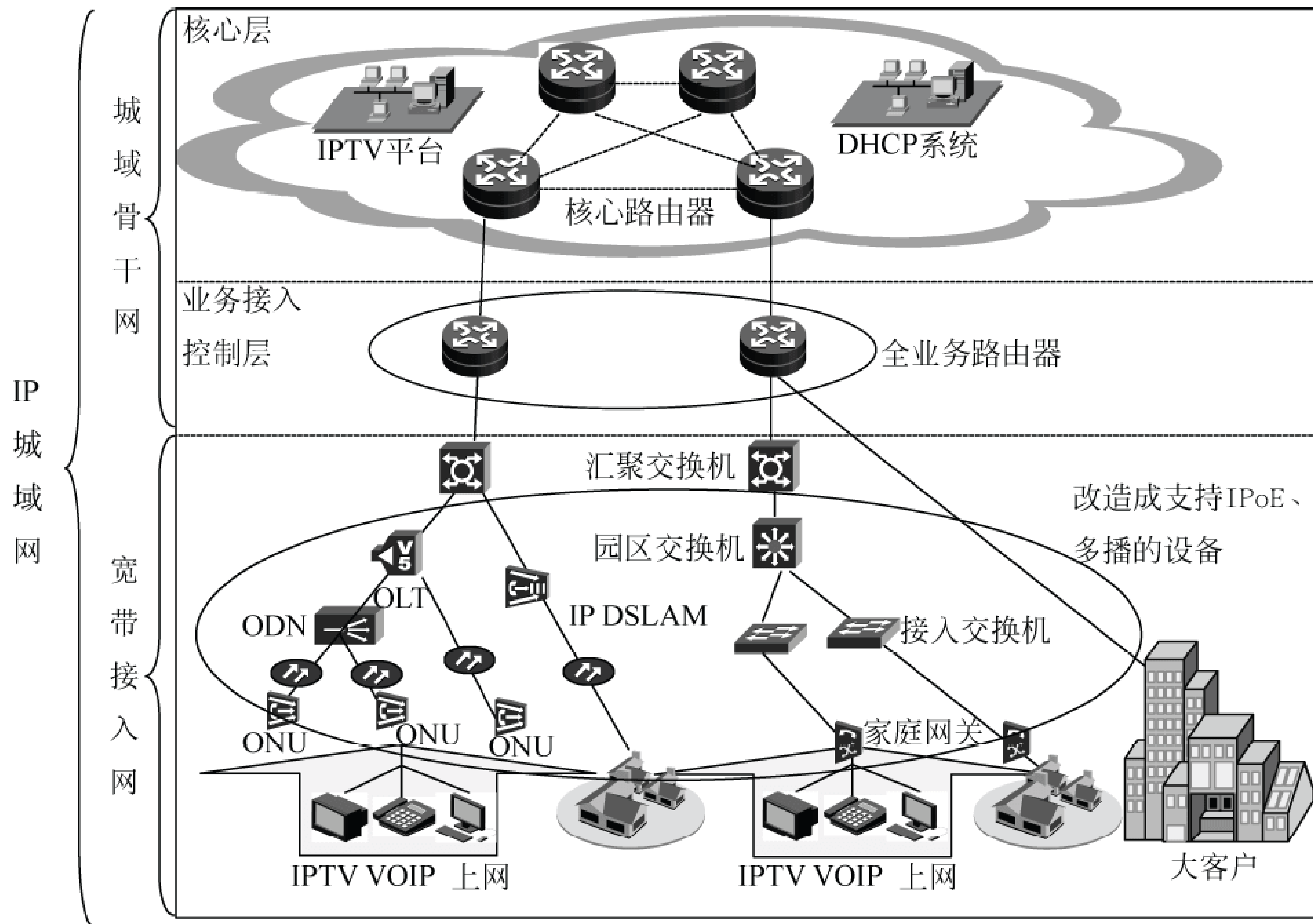
【问题 3】

（1）

① 核心层的设备保持不变，在业务接入控制层根据不同的业务需求进行设备接入区分优化。将宽带接入服务器（BRAS）作为使用 PPPoE 上网业务的边缘控制设备，业务路由器（SR）作为使用 IPoE 的 IPTV、流媒体等关键业务的边缘控制设备，形成多边缘的网络架构。

② 宽带接入网主要将接入层设备改造成支持 IPoE 和多播的设备。接入层设备包括 OLT、EPON、园区交换机和楼道交换机等。

（2）



① 城域骨干网核心层的设备保持不变，在业务接入控制层选择新建全业务路由器，或升级现网 BRAS 为全业务网关来负责业务统一接入，具备 BRAS 和 SR 的功能，形成单边缘的网络架构；

② 宽带接入网主要将接入层设备改造成支持 IPoE 的设备。接入层设备包括 OLT、EPON、园区交换机和楼道交换机等。

（3）

多边缘的网络架构：

优点：现网结构保持不变或改动小，投资较小；上网业务和视频等业务区分接入，可满足不同业务的需求。

缺点：多边缘的网络架构存在多张计费清单，存在同步等问题；对接入层设备要求高，需对不同业务做分离，接入层 QoS 策略复杂。

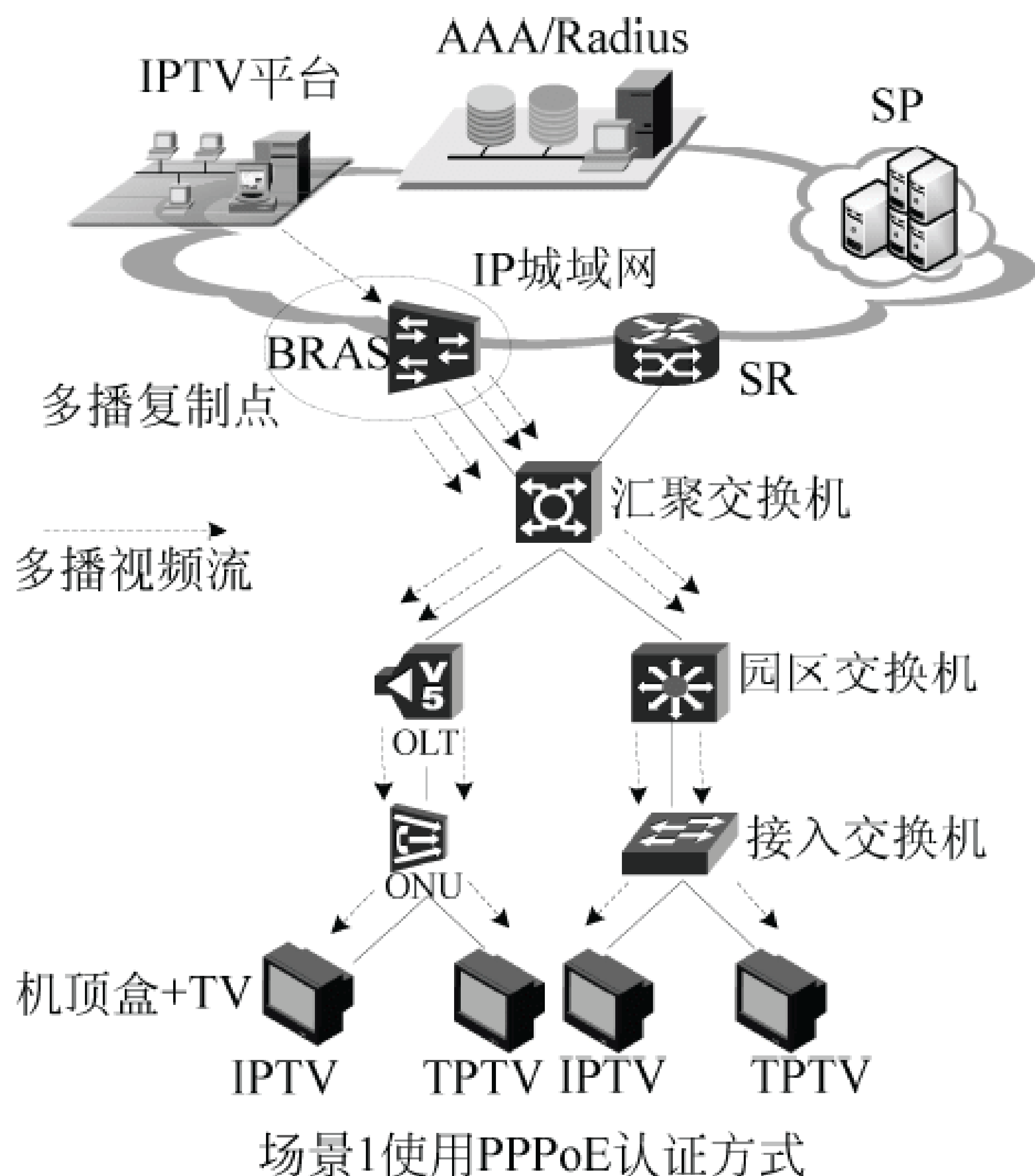
单边缘的网络架构：

优点：全业务统一接入，便于业务管理；简化了业务控制层的结构及设备维护；简化接入层 QoS 的策略部署。

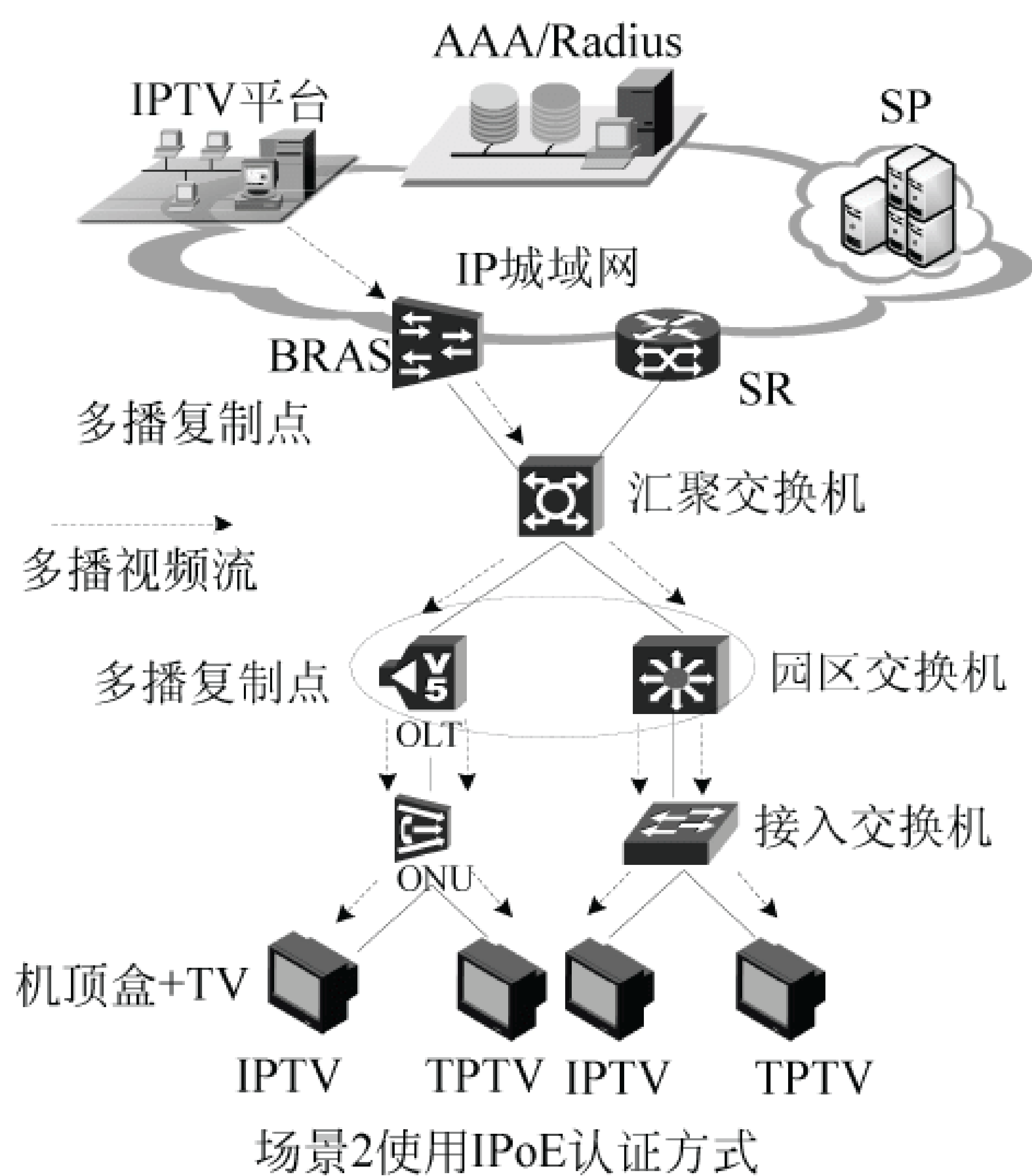
缺点：现网结构改动大，投资大。

【问题 4】

（1）



场景1使用PPPoE认证方式



场景2使用IPoE认证方式

① 使用 PPPoE 认证，IPTV 的多播复制点只能是 BRAS。

如场景 1 所示，多播复制点为 BRAS，BRAS 面向每个 IPTV 用户都要复制一份数据。这种场景对 BRAS 下行链路（BRAS—汇聚交换机）的带宽，园区交换机、OLT 的上行链路（园区交换机、OLT—汇聚交换机）的带宽及 IP 城域网带宽资源造成很大的压力。

② 使用 IPoE 认证，IPTV 的多播复制点可以灵活选择在 OLT、IP DSLAM、汇聚交换机、园区交换机、接入交换机。

如场景 2 所示，多播复制点为园区交换机和 OLT，由园区交换机、OLT 面向每个 IPTV 用户进行数据复制。大大节省了带宽资源，降低 BRAS 压力。

（2）根据上述比较，在 IPTV 发展初期，用户规模比较小时，运营商往往采用 BRAS 接入，通过 PPPoE 协议认证。随着用户规模的逐步扩大，PPPoE 的缺点逐渐显露，加之建设成本高。因此，在 IPTV 业务快速发展时，运营商宜采用 IPoE 方式承载 IPTV。

试题三（共 25 分）

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

【说明】

图 3-1 是某制造企业网络拓扑，该网络包括制造生产、研发设计、管理及财务、服务器群和销售部等五个部分。该企业通过对路由器的配置、划分 VLAN、使用 NAT 技术以及配置 QoS 与 ACL 等实现对企业网络的安全防护与管理。

随着信息技术与企业信息化应用的深入融合，一方面提升了企业的管理效率，同时企业在经营中面临的网络安全风险也在不断增加。为了防范网络攻击、保护企业重要信息数据，企业重新制定了网络安全规划，提出了改善现有网络环境的几项要求：

1．优化网络拓扑，改善网络影响企业安全运行的薄弱环节；
2．分析企业网络，防范来自外部攻击，制定相应的安全措施；
3．重视企业内部控制管理，制定技术方案，降低企业重要数据信息的泄露风险；
4．在保证 IT 投资合理的范围，解决远程用户安全访问企业网络的问题；
5．制定和落实对服务器群安全管理的企业内部标准。

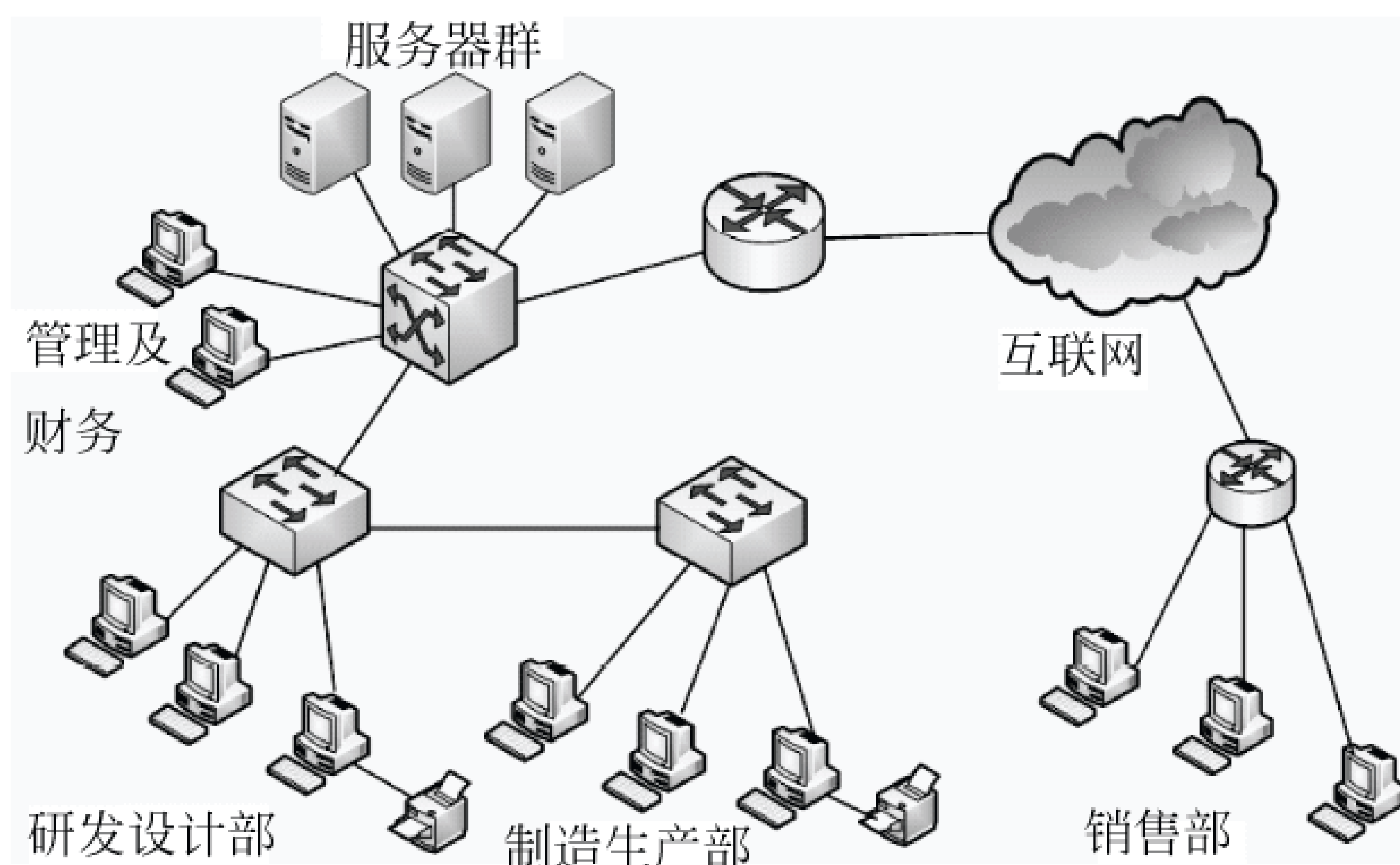


图 3-1

【问题 1】（5 分）

请分析说明该企业现有的网络安全措施是如何规划与部署的，应从哪些角度实现对

网络的安全管理。

【问题 2】（5 分）

请分析说明该企业的网络拓扑是否存在安全隐患，原有网络设备是否可以有效防御外来攻击。

【问题 3】（5 分）

入侵检测系统（IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。请简要说明该企业部署 IDS 的必要性以及如何在该企业网络中部署 IDS。

【问题 4】（5 分）

销售部用户接入企业网采用 VPN 的方式，数据通过安全的加密隧道在公共网络中传播，具有节省成本、安全性高、可以实现全面控制和管理等特点。简要说明 VPN 采用了哪些安全技术以及主要的 VPN 隧道协议有哪些。

【问题 5】（5 分）

请结合自己做过的案例，说明在进行企业内部服务器群的安全规划时需要考虑哪些因素。

试题三分析

本题考查局域网络安全的相关知识，包括 NAT、VLAN、GAP(网闸)、ACL、VPN 等的综合运用以及网络安全拓扑的规划、管理等内容。

【问题 1】

该企业现有的网络需要进行多级的安全部署。首先在接入层交换机上进行访问控制；采用 VLAN 技术通过用户隔离，实现对敏感信息的访问进行限制；在边界路由器上配置 NAT，屏蔽内网地址信息，降低外部的攻击；边界路由器上配置 ACL 访问控制列表，可以实现策略控制，进行访问权限控制。

【问题 2】

该企业现有的网络存在诸多安全隐患：

1. 制造生产部子网络应该直接接入核心交换机，该网络中当研发部子网络的交换设备故障时将会直接对制造生产部的一线产生影响；

2. 在内部网和外部网之间、专用网与公共网之间没有专门的防护设备，不能防御外来攻击；

3. 服务器群应设置在防火墙的 DMZ 区；

4. 应当配备 IPS 设备、流量监控、上网行为管理和网络病毒防护设备；

5. 采用网闸物理隔离财务部门和有关涉密部门。GAP 全称安全隔离网闸。安全隔离网闸是一种由带有多种控制功能专用硬件在电路上切断网络之间的链路层连接，并能够在网络间进行安全适度的应用数据交换的网络安全设备。

【问题 3】

入侵检测系统（IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。通常 IDS 采用旁路方式接入核心交换机，可以和防火墙互为补充，防止内部人员攻击，攻击发生后的取证等。

【问题 4】

VPN（虚拟专用网络）是指在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 有多种分类方式，主要是按协议进行分类。VPN 可通过服务器、硬件、软件等多种方式实现，VPN 具有成本低，易于使用的特点。主要采用的协议有：在互联网上建立 IP虚拟专用网隧道的协议 PPTP；建立在点对点协议 PPP 的基础上，把各种网络协议（IP、IPX 等）封装到 PPP 帧中，再把整个数据帧装入隧道协议 L2TP；对 IP 协议分组进行加密和认证的协议 IPSec。

【问题 5】

任何企业在做安全规划时，首先依据需求划分信息安全级别，然后依据安全级别，考虑 DMZ 区安全防护，机房的物理安全，主机的系统安全，数据备份机制，安全管理制度等等。

试题三参考答案

【问题 1】

1. 接入交换机上进行访问控制；
2. VLAN 技术通过用户隔离，实现对敏感信息的访问进行限制；
3. 在边界路由器上配置 NAT，屏蔽内网地址信息，降低外部的攻击；
4. 边界路由器上配置 ACL 访问控制列表，可以实现策略控制，进行访问权限控制。

【问题 2】

1. 制造生产部子网络应该直接接入核心交换机，该网络中当研发部子网络的交换设备故障时将会直接对制造生产部的一线产生影响；
2. 在内部网和外部网之间、专用网与公共网之间没有专门的防护设备，不能防御外来攻击；
3. 服务器群应设置在防火墙的 DMZ 区；
4. 应当配备 IPS 设备、流量监控、上网行为管理和网络病毒防护设备；
5. 采用网闸物理隔离财务部门和有关涉密部门。

【问题 3】

必要性：1．防止内部人员攻击；
2．和防火墙互为补充；
3．攻击发生后的取证。

部署：采用旁路方式接入核心交换机

【问题 4】

VPN 采用的安全隧道技术包括：加解密技术、密钥管理技术、身份认证技术。

VPN 协议有：PPTP、L2PT、IPSec。

【问题 5】

1. 首先划分信息安全级别
2. 依据安全级别，考虑以下内容：

（1）DMZ 区安全防护

（2）机房的物理安全

（3）主机的系统安全

（4）数据备份机制

（5）安全管理制度

第 21 章　2014 下半年网络规划设计师下午试题 II 写作要点

论题一　论网络中心机房的规划与设计

随着计算机的发展和网络的广泛应用，越来越多的单位建立了自己的网络，网络中心机房的建设是其中一个重要环节。它不仅集建筑、电气、安装、网络等多个专业技术于一体，更需要丰富的工程实施和管理经验。网络中心机房设计与施工的优劣直接关系到机房内计算机系统是否能稳定可靠地运行，是否能保证各类信息通信的畅通。

请围绕“论网络中心机房的规划与设计”论题，依次对以下三个方面进行论述。

1. 概要叙述你参与设计实施的网络项目以及你所担任的主要工作。
2. 具体讨论在网络中心机房的规划与设计中的主要工作内容和你所采用的原则、方法和策略，以及遇到的问题和解决措施。
3. 分析你所规划和设计网络中心机房的实际运行效果。你现在认为应该做哪些方面的改进以及如何加以改进。

写作要点

1. 机房工程整体建设。
2. 防静电地板铺设。
3. 隔断装修。
4. UPS 不间断电源。
5. 精密空调系统。
6. 新风换气系统。
7. 接地系统。
8. 防雷系统。
9. 监控系统。
10. 门禁系统。
11. 漏水检测系统。
12. 机房环境及动力设备监控系统。
13. 消防系统。
14. 屏蔽系统。

论题二　大型企业集团公司网络设计解决方案

公司为了发展业务、提高核心竞争能力，希望新建一个快捷安全的通信网络综合信息系统。该公司网络的基本需求如下：

1. 公司办公地点分布在多个地方。在 A 城市除了公司本部外还有一个相距 10 公里

的生产工厂，在相距 1000 公里外的 B 城市有一个研发部门，还有遍布全国 30 个大中城市的营销公司也需要联网。

2. 网络用户除固定的桌面系统外还有移动终端上网需求。

3. 公司本部包括经理办公室、生产部、市场部、人力资源部等多个办公部门，共有信息点 3000 个（不包括移动终端，下同），生产工厂和研发部也划分为一些科室，各有信息点 1000 个左右。

4. 建立一个符合开放性规范的综合业务通信网络，集成 OA 办公和企业管理，能够进行数据、声音、图像综合传输的网络平台。

5. 网络要符合下列要求：先进性、通用性和容错性，可扩展可升级，便于维护管理，性价比高。

请围绕“大型企业集团公司网络设计解决方案”论题，依次对以下四个方面进行论述。

1. 根据你自己参与的网络规划和建设项目，参考常见的网络设计方案，按照以上要求给出本网络的解决方案。

2. 描述网络连接拓扑结构、设备选型和地址分配等具体方案。

3. 概述网络安全解决方案，分析方案的优缺点及选择依据。

4.在实际网络设计项目中需重点解决的问题。

写作要点

一、网络拓扑结构图

二、设备选型

1．核心层交换机的选择

核心骨干设备的选择最为重要，要根据业务需求和未来发展规划，在 5 个重要的性能指标方面进行选择。

（1）网络接口类型：必须具有 10M/100M/1000M 端口。10G 以太网可以作为可选项，根据网络业务和未来发展规划确定是否必备。骨干以太网交换机大都支持广域网端口，并提供城域间网络连接，CWDM 支持也是设备选型时的重要参考。

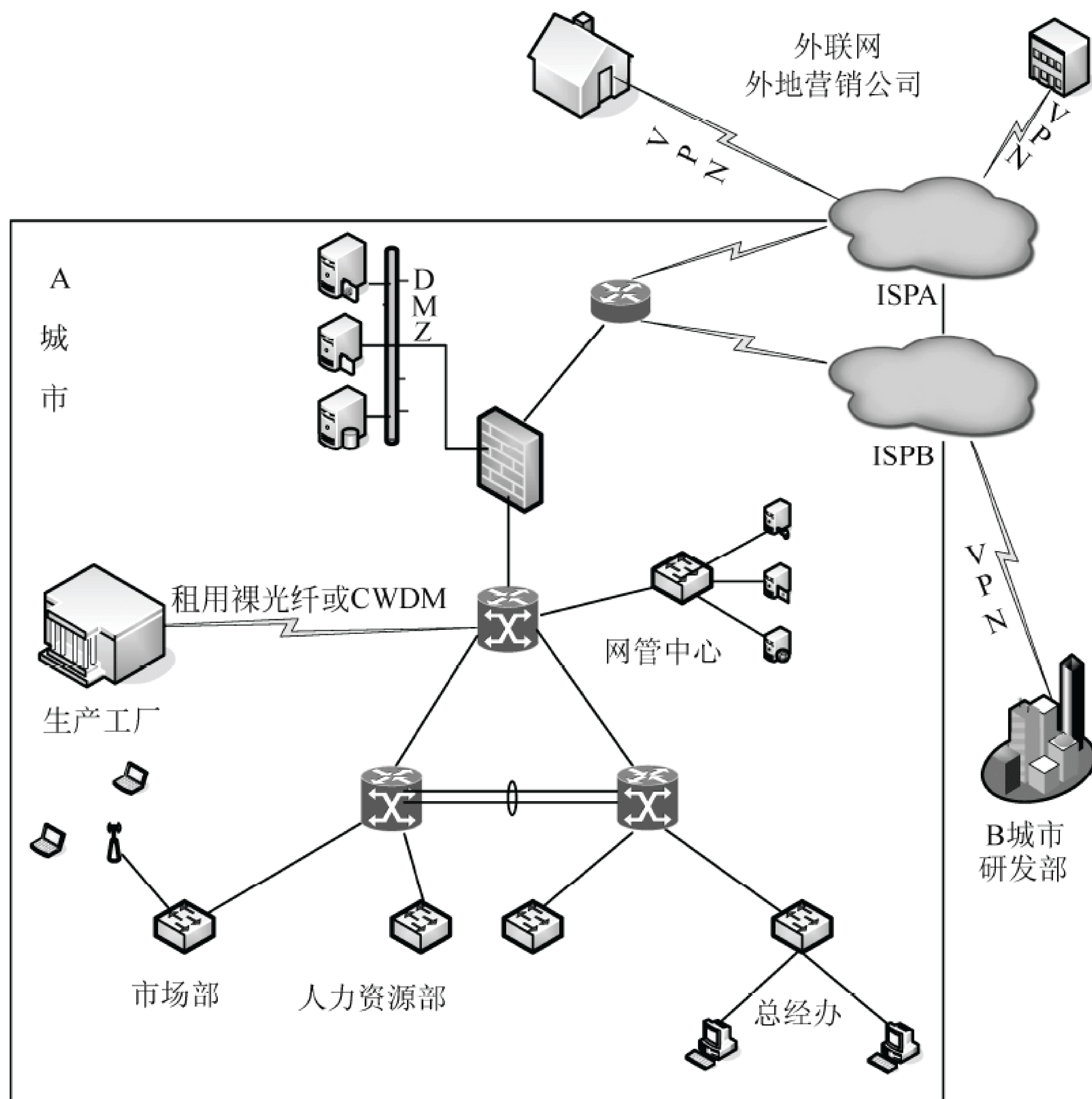
（2）吞吐量指标：吞吐量反映了交换机对数据包的拆分、封装、策略处理、转发/路由数据包的能力。核心交换设备的最高性能是无阻塞地实现数据交换，不仅应该提供二层以太帧的线速转发，而且应该提供三层数据包的线速转发。

（3）可用性指标：交换机是否支持关键模块（电源、风扇、交换矩阵、CPU 等）的冗余；链路层是否具备弹性恢复功能，网络层是否支持动态路由协议，是否支持等价多路由功能，是否支持网关冗余协议(VRRP)。

（4）单/组播协议：必须支持单播路由协议和多路广播路由协议。作为骨干交换机必须支持 RIPv1、RIPv2、OSPF 等路由协议，这些路由协议能够很好地互通，其他路由协议根据具体的需求来确定是否必需。

（5）QoS 保障：这是在网络拥塞时确保高优先级流量获得带宽的技术。由于关键的

多媒体应用大量涌现，要求交换机硬件支持优先级队列的数量越来越多，仅支持 2～3 个硬件优先级队列的产品已不能满足用户的业务需求。



当前市场上核心交换机比较常用的有锐捷网络系列核心路由交换机、Cisco Catalyst 6500 系列，D-Link DES-7600、D-Link DES-6500 等。

2．汇聚层交换机的选型

汇聚层交换机必须具有交换路由、可管理、高 QoS 保障、高安全性，以及支持多业务应用特性等功能。

可对网络及设备监控和管理。用户在选择交换机产品时，除了能满足对整个网络节点的拓扑发现、流量监控、状态监控等需求以外，还应对交换机提出远程配置、用户管理、访问控制乃至 QoS 监控等要求。

提供 QoS 保障功能。必须具有对不同应用类型数据进行分类处理（QoS）的功能，实现端到端的 QoS 保障，因而这要求交换机支持 802.1p 优先级、IntServ（RSVP）和 DiffServ 等功能。

要求汇聚交换机支持多媒体应用。整个网络的发展趋势是朝着网络融合以及应用融合的趋势发展，对于支持语音、组播等功能的交换机产品应优先考虑。

进行访问控制。网络变得越来越智能化，而在汇聚层设备上实现用户分类、权限设

置和访问控制是智能网络的重要功能。这就要求汇聚层设备能够支持 VLAN、AAA 技术（授权、认证、计费）、802.1x 等多种安全认证方式。

高安全性。为确保核心交换机不受类似拒绝服务（DoS）等攻击而导致全网瘫痪，不但要在核心交换机中采用防火墙和 IDS 预防和检测攻击的技术，在汇聚层交换设备中也必须增加此项功能，更好地实现全网安全。

比较常见的汇聚层交换机有华为 Quidway S5000 系列、Quidway S5600 系列等，锐捷 RG-5700 系列、RG-S4009 系列等，Cisco Catalyst 4500 系列、Cisco Catalyst 3700 系列等。

中低端交换机的生产厂商很多，主要有 Cisco（思科）、Juniper（杰科）、H3C（华为 3COM）、中兴通信等公司。

3．防火墙产品的选择

防火墙是在内部网和外部网之间、专用网与公共网之间构造的保护屏障，它是计算机硬件和软件的结合，从而保护内部网免受非法用户的入侵。防火墙主要由服务访问策略、验证工具、包过滤和应用网关 4 个部分组成。

以防火墙所采用的技术不同来区分，可分为：①包过滤型；②代理型；③监测型。

新一代监测型防火墙能够对各层数据包进行主动的、实时的监测，有效地判断各层中的非法侵入。同时，检测型防火墙一般还带有分布式探测器，这些探测器部署在各种应用服务器和各个网络节点之中，不仅能够检测来自网络外部的攻击，同时对来自内部的恶意破坏也有极强的防范作用。例如 CISCO ASA5505-UL-BUN-K8。

4．路由器的选型

根据下列指标进行选择：

（1）路由协议

路由器是用来连接不同网络的，这些不同的网络可能采用不同的路由协议。这就要求在选配路由器时注意它所支持的网络协议有哪些，特别是对于广域网中的路由器。

（2）背板能力

通常是指路由器背板容量或总线带宽。中档路由器的包转发能力均应在 1Mpps 以上。这个性能对于保证整个网络之间的连接速度是非常重要的。

（3）丢包率

丢包率是指在一定的数据流量下，路由器不能正确进行转发的数据包在总数据包中所占的比例。正常工作的路由器丢包率应小于 1%。

（4）转发延迟

路由器的转发延迟指从转发的数据包最后一比特进入路由器端口，到该数据包第一比特出现在出口链路上的时间间隔，通常用毫秒计算。这个参数通常在路由器端口吞吐量范围内进行测试。

（5）路由表容量

路由表容量是指路由器运行中可以容纳的路由数量。一般来说，路由器越高档，路由表容量越大。这一参数与路由器自身所带的缓存大小有关。

（6）可靠性

可靠性是指路由器的可用性、无故障工作时间和平均故障修复时间等指标，这一指标对新买的路由器无法验证。所以应该选择信誉较好、技术先进的品牌。

（7）网管能力

在大型网络中，路由器支持标准的网管系统尤为重要。一般的路由器厂商都会提供一些与之配套的网络管理系统软件。选择路由器时，务必要关注网络系统的监管和配置能力是否强大，设备是否可以提供统计信息和深层故障检测的诊断功能等。

三、地址分配方案

入口路由器进行 NAT 地址变换；通过 DHCP 服务器分配内部私网地址；每个二级单位组成一个 VLAN，地址空间分配如下：

10.0.0.0/8　　集团公司全部地址空间
10.16.0.0/13　　集团公司本部全部地址空间
10.16.64.0/17　　集团公司网管类全部地址
10.16.128.0/17　　集团公司互联类全部地址
10.16.196.0/17　　集团公司应用类全部地址
10.16.196.0 /21　　集团公司总经办地址空间
10.16.200.0/21　　集团公司生产部地址空间
10.16.204.0/21　　集团公司市场部地址空间
10.16.208.0/21　　集团公司后勤部地址空间
10.16.212.0/21　　集团公司人力资源部地址空间
10.16.216.0/21　　……………………地址空间
10.16.220.0/21　　……………………地址空间
10.16.224.0/21　　……………………地址空间

四、网络安全解决方案

设置防火墙保护内部网络免受非法用户的入侵；旁路接入 IDS 和 IPS 设备，监测网络入侵以及网络病毒的危害；在汇聚交换机上安装用户上网行为管理设备和流量监测设备；采用安全有效的用户认证方案，结合 Windows 域用户管理和审计功能，严格实施网络资源的访问控制。

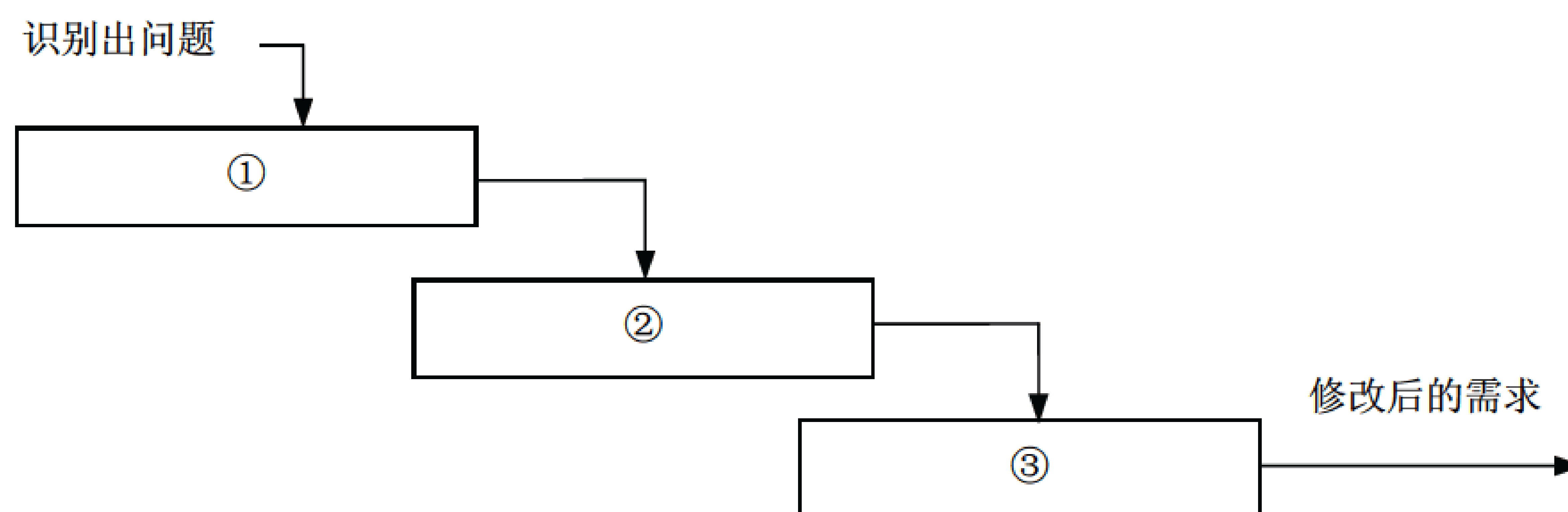
五、重点解决的问题

根据自己熟悉的领域，在需求分析、设备选型、网络安全解决方案等方面进行略微详细的论述。

第 22 章　2015 下半年网络规划设计师上午试题分析与解答

试题（1）、（2）

一个大型软件系统的需求总是有变化的。为了降低项目开发的风险，需要一个好的变更控制过程。如下图所示的需求变更管理过程中，①②③处对应的内容应是__（1）__；自动化工具能够帮助变更控制过程更有效地运作，__（2）__是这类工具应具有的特性之一。

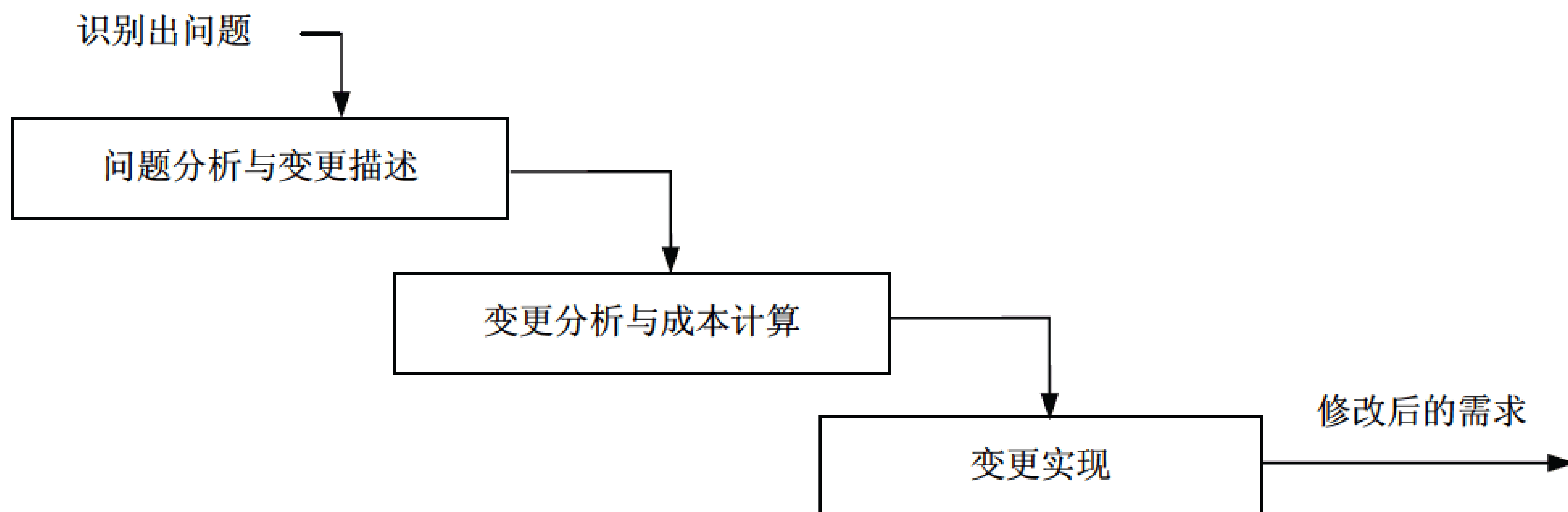


（1）A．问题分析与变更描述、变更分析与成本计算、变更实现
　　B．变更描述与变更分析、成本计算、变更实现
　　C．问题分析与变更描述、变更分析、变更实现
　　D．变更描述、变更分析、变更实现

（2）A．自动维护系统的不同版本
　　B．支持系统文档的自动更新
　　C．自动判定变更是否能够实施
　　D．记录每一个状态变更的日期和做出这一变更的人

试题（1）、（2）分析

一个大型的软件系统的需求总是有变化的。对许多项目来说，系统软件总需要不断完善，一些需求的改进是合理的而且不可避免，要使得软件需求完全不变更，也许是不可能的，但毫无控制的变更是项目陷入混乱、不能按进度完成，或者软件质量无法保证的主要原因之一。一个好的变更控制过程，给项目风险承担者提供了正式的建议需求变更机制，可以通过变更控制过程来跟踪已建议变更的状态，使已建议的变更确保不会丢失或疏忽。需求变更管理过程如下图所示：



① 问题分析和变更描述。这是识别和分析需求问题或者一份明确的变更提议，以检查它的有效性，从而产生一个更明确的需求变更提议。

② 变更分析和成本计算。使用可追溯性信息和系统需求的一般知识，对需求变更提议进行影响分析和评估。变更成本计算应该包括对需求文档的修改、系统修改的设计和实现的成本。一旦分析完成并且确认，应该进行是否执行这一变更的决策。

③ 变更实现。这要求需求文档和系统设计以及实现都要同时修改。如果先对系统的程序做变更，然后再修改需求文档，这几乎不可避免地会出现需求文档和程序的不一致。

自动化工具能够帮助变更控制过程更有效地运作。许多团队使用商业问题跟踪工具来收集、存储和管理需求变更。用这样的工具创建的最近提交的变更建议清单，可以用作 CCB 会议的议程。问题跟踪工具也可以随时按变更状态分类报告出变更请求的数目。

因为可用的工具、厂商和特性总在频繁地变化，所以这里无法给出有关工具的具体建议。但工具应该具有以下几个特性，以支持需求变更过程：

① 可以定义变更请求中的数据项；

② 可以定义变更请求生命周期的状态转换模型；

③ 可以强制实施状态转换模型，以便只有授权用户可以做出允许的状态变更；

④ 可以记录每一个状态变更的日期和做出这一变更的人；

⑤ 可以定义当提议者提交新请求或请求状态被更新时，哪些人可以自动接收电子邮件通知；

⑥ 可以生成标准的和定制的报告和图表。

有些商业需求管理工具内置有简单的变更建议系统。这些系统可以将提议的变更与某一特定的需求联系起来，这样无论什么时候，只要有人提交了一个相关的变更请求，负责需求的每个人都会收到电子邮件通知。

参考答案

（1）A　　（2）D

试题（3）

用例（use case）用来描述系统对事件做出响应时所采取的行动。用例之间是具有相

关性的。在一个会员管理系统中，会员注册时可以采用电话和邮件两种方式。用例“会员注册”、“电话注册”与 “邮件注册”之间是＿（3）＿关系。

（3）A．包含（include）　　B．扩展（extend）

C．泛化（generalize）　　D．依赖（depends on）

试题（3）分析

用例之间的关系主要有包含、扩展和泛化，利用这些关系，把一些公共的信息抽取出来，以便于复用，使得用例模型更易于维护。

① 包含关系。当可以从两个或两个以上的用例中提取公共行为时，应该使用包含关系来表示它们。其中这个提取出来的公共用例称为抽象用例，而把原始用例称为基本用例或基础用例。

② 扩展关系。如果一个用例明显地混合了两种或两种以上的不同场景，即根据情况可能发生多种分支，则可以将这个用例分为一个基本用例和一个或多个扩展用例，这样使描述可能更加清晰。

③ 泛化关系。当多个用例共同拥有一种类似的结构和行为的时候，可以将它们的共性抽象成为父用例，其他的用例作为泛化关系中的子用例。在用例的泛化关系中，子用例是父用例的一种特殊形式，子用例继承了父用例所有的结构、行为和关系。

参考答案

（3）C

试题（4）、（5）

RUP 强调采用＿（4）＿的方式来开发软件，这样做的好处是＿（5）＿。

（4）A．原型和螺旋　　B．螺旋和增量　　C．迭代和增量　　D．快速和迭代

（5）A．在软件开发的早期就可以对关键的、影响大的风险进行处理

B．可以避免需求的变更

C．能够非常快速地实现系统的所有需求

D．能够更好地控制软件的质量

试题（4）、（5）分析

RUP 将项目管理、业务建模、分析与设计等统一起来，贯穿整个开发过程。RUP 中的软件过程在时间上被分解为 4 个顺序的阶段，分别是初始阶段、细化阶段、构建阶段和移交阶段。每个阶段结束时都要安排一次技术评审，以确定这个阶段的目标是否已经满足。如果评审结果令人满意，就可以允许项目进入下一个阶段。可以看出，基于 RUP 的软件过程是一个迭代和增量的过程。通过初始、细化、构建和移交 4 个阶段就是一个开发周期，每次经过这 4 个阶段就会产生一代软件。除非产品退役，否则通过重复同样的 4 个阶段，产品将演化为下一代产品，但每一次的侧重点都将放在不同的阶段上。这样做的好处是在软件开发的早期就可以对关键的、影响大的风险进行处理。

参考答案

（4）C　　（5）A

试题（6）、（7）

__（6）__的目的是检查模块之间，以及模块和已集成的软件之间的接口关系，并验证已集成的软件是否符合设计要求；其测试的技术依据是__（7）__。

（6）A．单元测试　B．集成测试　C．系统测试　D．回归测试

（7）A．软件详细设计说明书　B．技术开发合同

C．软件概要设计文档　D．软件配置文档

试题（6）、（7）分析

根据国家标准 GB/T 15532-2008，软件测试可分为单元测试、集成测试、配置项测试、系统测试、验收测试和回归测试等类别。

单元测试也称为模块测试，测试的对象是可独立编译或汇编的程序模块、软件构件或面向对象软件中的类（统称为模块），其目的是检查每个模块能否正确地实现设计说明中的功能、性能、接口和其他设计约束等条件，发现模块内可能存在的各种差错。单元测试的技术依据是软件详细设计说明书。

集成测试的目的是检查模块之间，以及模块和已集成的软件之间的接口关系，并验证已集成的软件是否符合设计要求。集成测试的技术依据是软件概要设计文档。

系统测试的对象是完整的、集成的计算机系统，系统测试的目的是在真实系统工作环境下，验证完整的软件配置项能否和系统正确连接，并满足系统/子系统设计文档和软件开发合同规定的要求。系统测试的技术依据是用户需求或开发合同。

配置项测试的对象是软件配置项，配置项测试的目的是检验软件配置项与软件需求规格说明的一致性。

确认测试主要验证软件的功能、性能和其他特性是否与用户需求一致。

验收测试是指针对软件需求规格说明，在交付前以用户为主进行的测试。

回归测试的目的是测试软件变更之后，变更部分的正确性和对变更需求的复合型，以及软件原有的、正确的功能、性能和其他规定的要求的不损害性。

参考答案

（6）B　　（7）C

试题（8）

甲、乙、丙、丁四人加工 A、B、C、D 四种工件所需工时如下表所示。指派每人加工一种工件，四人加工四种工件其总工时最短的最优方案中，工件 B 应由__（8）__加工。

	A	B	C	D
甲	14	9	4	15
乙	11	7	7	10
丙	13	2	10	5
丁	17	9	15	13

（8）A. 甲　　B. 乙　　C. 丙　　D. 丁

试题（8）分析

本题考查数学（运筹学）应用的能力。

本题属于指派问题：要求在 4×4 矩阵中找出四个元素，分别位于不同行、不同列，使其和达到最小值。

显然，任一行（或列）各元素都减（或加）一常数后，并不会影响最优解的位置，只是目标值（指派方案的各项总和）也减（或加）了这一常数。

我们可以利用这一性质使矩阵更多的元素变成 0，其他元素保持正，以利于求解。

$$\begin{pmatrix} 14 & 9 & 4 & 15 \\ 11 & 7 & 7 & 10 \\ 13 & 2 & 10 & 5 \\ 17 & 9 & 15 & 13 \end{pmatrix} \xrightarrow[\text{第 3 列都减 4 \quad 第 4 列都减 5 得}]{\text{第 1 列都减 11 \quad 第 2 列都减 2}} \begin{pmatrix} 3 & 7 & 0 & 10 \\ 0 & 5 & 3 & 5 \\ 2 & 0 & 6 & 0 \\ 6 & 7 & 11 & 8 \end{pmatrix}$$

$$\xrightarrow{\text{第 4 行都减 6 得}} \begin{pmatrix} 3 & 7 & 0 & 10 \\ 0 & 5 & 3 & 5 \\ 2 & 0 & 6 & 0 \\ 0 & 1 & 5 & 2 \end{pmatrix}$$

。累计减数 11+2+4+5+6=28。

对该矩阵，并不存在全 0 指派。位于(1，3)、(2，1)、(3，4)、(4，2)的元素之和为 1 是最小的。因此，分配甲、乙、丙、丁分别加工 C、A、D、B 能达到最少的总工时 28+1=29。

更进一步，再在第三行上都加 1，在第 2、4 列上都减 1，可得到更多的 0 元素：

$$\begin{pmatrix} 3 & 6 & 0 & 9 \\ 0 & 4 & 3 & 4 \\ 3 & 0 & 7 & 0 \\ 0 & 0 & 5 & 1 \end{pmatrix}$$

，这样就断定上述位置是唯一的全 0（最优）指派。

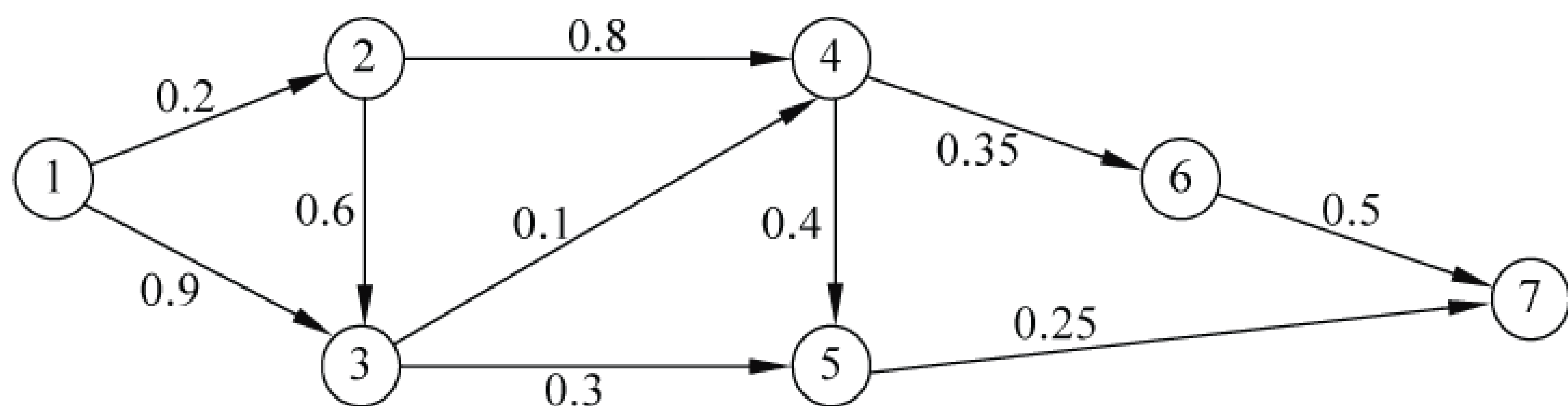
本题也可用试验法解决，但比较烦琐，需要仔细，不要遗漏。

参考答案

（8）D

试题（9）

小王需要从①地开车到⑦地，可供选择的路线如下图所示。图中，各条箭线表示路段及其行驶方向，箭线旁标注的数字表示该路段的拥堵率（描述堵车的情况，即堵车概率）。拥堵率=1−畅通率，拥堵率=0 时表示完全畅通，拥堵率=1 时表示无法行驶。根据该图，小王选择拥堵情况最少（畅通情况最好）的路线是__（9）__。

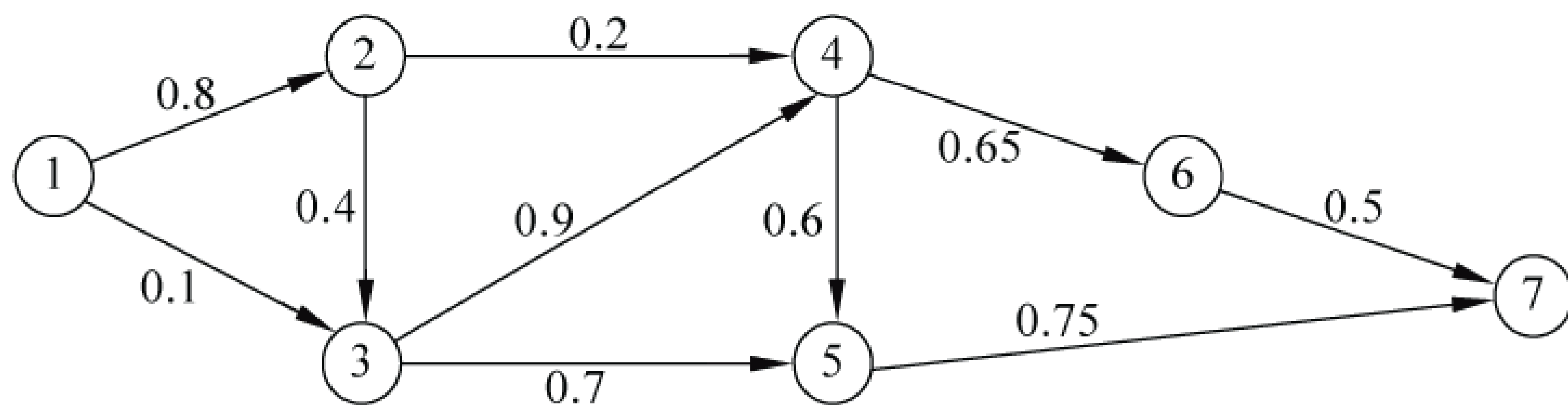


（9）A. ①②③④⑤⑦　　B. ①②③④⑥⑦
　　C. ①②③⑤⑦　　D. ①②④⑥⑦

试题（9）分析

本题考查数学（概率）应用的能力。

首先将路段上的拥堵率转换成畅通率如下图：



每一条路线上的畅通率等于所有各段畅通率之乘积。两点之间的畅通率等于两点之间所有可能路线畅通率的最大值。以下用 T（ijk…）表示从点 i 出发，经过点 j、k…等的路线的畅通率。

据此原则，可以从①开始逐步计算到达各点的最优路线。

T（①②）= 0.8；　　对应路线①②

T（①③）= max（0.1，0.8×0.4）=0.32；　　对应路线①②③

T（①④）= max（0.8×0.2，0.32×0.9）=0.288；　　对应路线①②③④

T（①⑤）= max（0.32×0.7，0.288×0.6）=0.224；　　对应路线①②③⑤

T（①⑥）= 0.224×0.65=0.1456；　　对应路线①②③⑥

T（①⑦）=max（0.1456×0.5，0.224×0.75）=0.168。　　对应路线①②③⑤⑦

结论：小王应选择路线①②③⑤⑦，该线路有最好的畅通率 0.168，或最小的拥堵率 0.832。

参考答案

（9）C

试题（10）

软件设计师王某在其公司的某一综合信息管理系统软件开发项目中承担了大部分程序设计工作。该系统交付用户，投入试运行后，王某辞职离开公司，并带走了该综合信息管理系统的源程序，拒不交还公司。王某认为综合信息管理系统源程序是他独立完成的，他是综合信息管理系统源程序的软件著作权人。王某的行为__（10）__。

（10）A. 侵犯了公司的软件著作权　　B. 未侵犯公司的软件著作权
　　C. 侵犯了公司的商业秘密权　　D. 不涉及侵犯公司的软件著作权

试题（10）分析

本题考查知识产权基本知识。

《计算机软件保护条例》第 13 条规定“自然人在法人或者其他组织中任职期间所开发的软件有下列情形之一的，该软件著作权由该法人或者其他组织享有，该法人或者其

他组织可以对开发软件的自然人进行奖励：

（一）针对本职工作中明确指定的开发目标所开发的软件；

（二）开发的软件是从事本职工作活动所预见的结果或者自然的结果；

（三）主要使用了法人或者其他组织的资金、专用设备、未公开的专门信息等物质技术条件所开发并由法人或者其他组织承担责任的软件。”

根据《计算机软件保护条例》规定，可以得出这样的结论，当公民作为某单位的职工时，如果其开发的软件属于执行本职工作的结果，该软件著作权应当归单位享有。而单位可以给予开发软件的职工奖励。需要注意的是，奖励软件开发者并不是单位的一种法定义务，软件开发者不可援引《计算机软件保护条例》强迫单位对自己进行奖励。

王某作为公司的职员，完成的某一综合信息管理系统软件是针对其本职工作中明确指定的开发目标而开发的软件。该软件应为职务作品，并属于特殊职务作品。公司对该软件享有除署名权外的软件著作权的其他权利，而王某只享有署名权。王某持有该软件源程序不归还公司的行为，妨碍了公司正常行使软件著作权，构成对公司软件著作权的侵犯，应承担停止侵权责任，即交还软件源程序。

参考答案

（10）A

试题（11）

下面的网络中不属于分组交换网的是__（11）__。

（11）A．ATM　　B．POTS　　C．X.25　　D．IPX/SPX

试题（11）分析

ATM 网络是分组交换网，交换的单元是信元；X.25 是分组交换网，交换的单元是 X.25 分组；IPS/SPX 也是分组交换网，在网络层交换的是 IPX 分组。只有 POTS（Plain Old Telephone Service，普通老式电话业务）不是分组交换网，这种网络中传输的是用模拟信号表示的语音流。

参考答案

（11）B

试题（12）、（13）

ADSL 采用__（12）__技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供话音和联网服务，ADSL2+技术可提供的最高下行速率达到__（13）__Mb/s。

（12）A．时分复用　　B．频分复用　　C．空分复用　　D．码分多址

（13）A．8　　B．16　　C．24　　D．54

试题（12）、（13）分析

ADSL 采用频分复用技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供话音和联网服务，ADSL2+技术可提供的最高下行速率达到 24Mb/s。

参考答案

（12）B （13）C

试题（14）、（15）

下面 4 组协议中，属于第二层隧道协议的是__（14）__。第二层隧道协议中必须要求 TCP/IP 支持的是__（15）__。

（14）A．PPTP 和 L2TP　　B．PPTP 和 IPSec
　　C．L2TP 和 GRE　　D．L2TP 和 IPSec

（15）A．IPSec　　B．PPTP　　C．L2TP　　D．GRE

试题（14）、（15）分析

PPTP 和 L2TP 都属于第二层隧道协议，PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加包头用于在互联网络上传输。两个协议存在以下几方面的区别。

① PPTP 要求因特网络为 IP 网络，L2TP 只要求隧道媒介提供面向数据包的点对点连接。L2TP 可以在 IP（使用 UDP）、帧中继永久虚拟电路（PVCs）、X.25 虚电路（VCs）或 ATM 网络上使用。

② PPTP 只能在两端点间建立单一隧道，L2TP 支持在两端点间使用多个隧道。使用 L2TP，用户可以针对不同的服务质量创建不同的隧道。

③ L2TP 可以提供包头压缩。当压缩包头时，系统开销占用 4 个字节，而在 PPTP 协议下要占用 6 个字节。

④ L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是，当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第 2 层协议上验证隧道。

参考答案

（14）A （15）B

试题（16）～（18）

IP 数据报的分段和重装配要用到报文头部的标识符、数据长度、段偏置值和__（16）__等四个字段，其中__（17）__字段的作用是为了识别属于同一个报文的各个分段，__（18）__的作用是指示每一分段在原报文中的位置。

（16）A．IHL　　B．M 标志　　C．D 标志　　D．头校验和

（17）A．IHL　　B．M 标志　　C．D 标志　　D．标识符

（18）A．段偏置值　　B．M 标志　　C．D 标志　　D．头校验和

试题（16）～（18）分析

在 DoD 和 ISO 的 IP 协议中使用了 4 个字段处理分段和重装配问题。一个是报文 ID 字段，它唯一地标识了某个站某一个协议层发出的数据。在 DoD 的 IP 协议中，ID 字段由源站和目标站地址、产生数据的协议层标识符以及该协议层提供的顺序号组成。第二个字段是数据长度，即字节数。第三个字段是偏置值，即分段在原来数据报中的位置，以 8 个字节（64 位）的倍数计数。最后是 M 标志，表示是否为最后一个分段。

当一个站发出数据报时对长度字段的赋值等于整个数据字段的长度，偏置值为 0，M 标志置为 False（用 0 表示）。如果一个 IP 模块要对该报文分段，则按以下步骤进行。

① 对数据块的分段必须在 64 位的边界上划分，因而除最后一段外，其他段长都是 64 位的整数倍。

② 对得到的每一分段都加上原来数据报的 IP 头，组成短报文。

③ 每一个短报文的长度字段置为它包含的字节数。

④ 第一个短报文的偏置值置为 0，其他短报文的偏置值为它前边所有报文长度之和（字节数）除以 8。

⑤ 最后一个报文的 M 标志置为 0（False），其他报文的 M 标志置为 1（True）。

参考答案

（16）B　（17）D　（18）A

试题（19）、（20）

TCP 使用的流量控制协议是__（19）__，TCP 段头中指示可接收字节数的字段是__（20）__。

（19）A．固定大小的滑动窗口协议　　B．可变大小的滑动窗口协议
　　　C．后退 N 帧 ARQ 协议　　D．停等协议

（20）A．偏置值　　B．窗口
　　　C．检查和　　D．接收顺序号

试题（19）、（20）分析

TCP 的流量控制机制是可变大小的滑动窗口协议，由接收方在窗口字段中指明接收缓冲区的大小。发送方发送了规定的字节数后等待接收方的下一次请求。固定大小的滑动窗口协议用在数据链路层的 HDLC 中。可变大小的滑动窗口协议可以应付长距离通信过程中线路延迟不确定的情况，而固定大小的滑动窗口协议则适合链路两端点之间通信延迟固定的情况。

参考答案

（19）B　（20）B

试题（21）、（22）

AAA 服务器（AAA Server）是一种处理用户访问请求的框架协议，它的主要功能有 3 个，但是不包括__（21）__，通常用来实现 AAA 服务的协议是__（22）__。

（21）A．身份认证　B．访问授权　C．数据加密　D．计费

（22）A．Kerberos　B．RADIUS　C．SSL　D．IPSec

试题（21）、（22）分析

AAA 服务器的主要目的是管理用户访问网络服务器权限，具体为：

1．验证（Authentication）：验证用户是否可以获得访问权限。

2．授权（Authorization）：授权用户可以使用哪些服务。

3．记账（Accounting）：记录用户使用网络资源的情况。

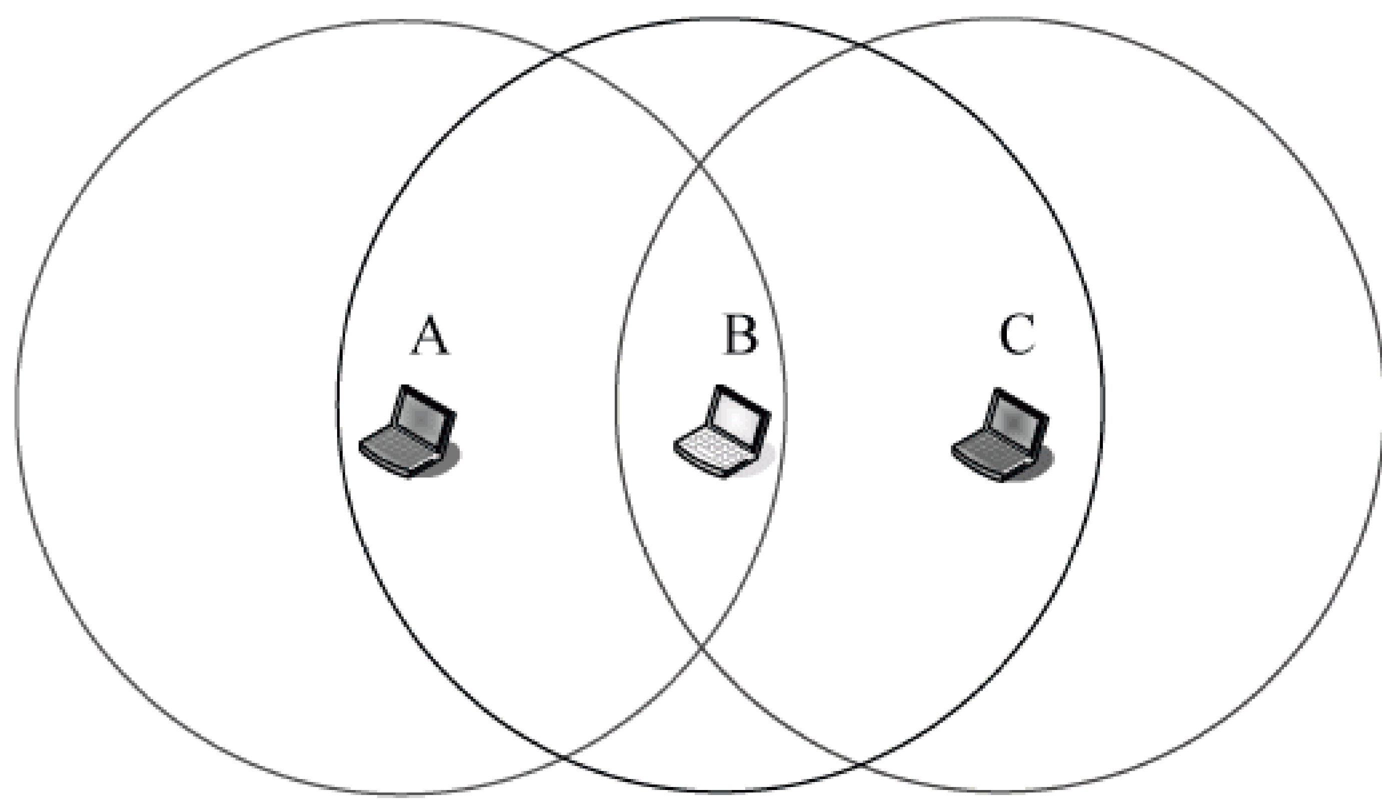
通常用来实现 AAA 服务的协议是RADIUS（Remote Authentication Dial In User Service）协议，这是基于 UDP 的一种客户机/服务器协议。RADIUS 客户机是网络访问服务器，它通常是一个路由器、交换机或无线访问点。RADIUS服务器通常是在 UNIX 或 Windows 2000 服务器上运行的一个监护程序。

参考答案

（21）C （22）B

试题（23）、（24）

由无线终端组成的 MANET 网络，与固定局域网最主要的区别是__（23）__。在下图所示的由 A、B、C 三个结点组成的 MANET 中，圆圈表示每个结点的发送范围，结点 A 和结点 C 同时发送数据，如果结点 B 不能正常接收，这时结点 C 称为结点 A 的__（24）__。



（23）A. 无线访问方式可以排除大部分网络入侵
B. 不需要运行路由协议就可以互相传送数据
C. 无线信道可以提供更大的带宽
D. 传统的路由协议不适合无线终端之间的通信

（24）A. 隐蔽终端 B. 暴露终端 C. 干扰终端 D. 并发终端

试题（23）、（24）分析

IEEE 802.11 标准定义的 Ad Hoc 网络是由无线移动结点组成的对等网，无须网络基础设施的支持，能够根据通信环境的变化实现动态重构，提供基于多跳无线连接的分组数据传输服务。在这种网络中，每一个结点既是主机，又是路由器，它们之间相互转发分组，形成一种自组织的 MANET（Mobile Ad Hoc Network）网络。

与传统的有线网络相比，MANET 有如下特点：

- 网络拓扑结构是动态变化的，由于无线终端的频繁移动，可能导致结点之间的相互位置和连接关系难以维持稳定。
- 无线信道提供的带宽较小，而信号衰落和噪声干扰的影响却很大。由于各个终端信号覆盖范围的差别，或者地形地物的影响，还可能存在单向信道。
- 无线终端携带的电源能量有限，应采用最节能的工作方式，因而要尽量减小网络通信开销，并根据通信距离的变化随时调整发射功率。

- 由于无线链路的开放性，容易招致网络窃听、欺骗、拒绝服务等恶意攻击的威胁，所以需要特别的安全防护措施。

路由算法是 MANET 网络中重要的组成部分，由于上述特殊性，传统有线网络的路由协议不能直接应用于 MANET。IETF 成立的 MANET 工作组开发了 MANET 路由规范，使其能够支持包含上百个路由器的自组织网络，并在此基础上开发支持其他功能的路由协议，例如支持节能、安全、组播、QoS 和 IPv6 的路由协议。

无线移动自组织网络中有一种特殊的现象，这就是隐蔽终端和暴露终端问题。在本题的图中，如果结点 A 向结点 B 发送数据，则由于结点 C 检测不到 A 发出的载波信号，它若试图发送，就可能干扰结点 B 的接收。所以对 A 来说，C 是隐蔽终端。另一方面，如果结点 B 要向结点 A 发送数据，它检测到结点 C 正在发送，就可能暂缓发送过程。但实际上 C 发出的载波不会影响 A 的接收，在这种情况下，结点 C 就是暴露终端。这些问题不但会影响数据链路层的工作状态，也会对路由信息的及时交换以及网络重构过程造成不利影响。

参考答案

（23）D　（24）A

试题（25）、（26）

移动通信 4G 标准与 3G 标准最主要的区别是<u>（25）</u>，当前 4G 标准有<u>（26）</u>。

（25）A．4G 的数据速率更高，而 3G 的覆盖范围更大
B．4G 是针对多媒体数据传输的，而 3G 只能传送话音信号
C．4G 是基于 IP 的分组交换网，而 3G 是针对语音通信优化设计的
D．4G 采用正交频分多路复用技术，而 3G 系统采用的是码分多址技术

（26）A．UMB 和 WiMAX II　　B．LTE 和 WiMAX II
C．LTE 和 UMB　　D．TD-LTE 和 FDD-LTE

试题（25）、（26）分析

移动通信 4G 标准与 3G 标准最主要的区别是：4G 是基于 IP 的分组交换网，而 3G 是针对语音通信优化设计的，当前 4G 标准有 LTE 和 WiMAX II。

参考答案

（25）C　（26）B

试题（27）、（28）

在从 IPv4 向 IPv6 过渡期间，为了解决 IPv6 主机之间通过 IPv4 网络进行通信的问题，需要采用<u>（27）</u>，为了使得纯 IPv6 主机能够与纯 IPv4 主机通信，必须使用<u>（28）</u>。

（27）A．双协议栈技术　　B．隧道技术
C．多协议栈技术　　D．协议翻译技术

（28）A．双协议栈技术　　B．隧道技术
C．多协议栈技术　　D．协议翻译技术

试题（27）、（28）分析

IETF 的 NGTRANS 工作组研究了从 IPv4 向 IPv6 过渡的问题，提出了一系列的过渡技术和互连方案。过渡初期要解决的问题可以分成两类：第一类是解决 IPv6 孤岛之间互相通信的问题，第二类是解决 IPv6 孤岛与 IPv4 海洋之间的通信问题。目前提出的过渡技术可以归纳为以下 3 种：

① 隧道技术：用于解决 IPv6 结点之间通过 IPv4 网络进行通信的问题；

② 双协议栈技术：使得 IPv4 和 IPv6 可以共存于同一设备和同一网络中；

③ 翻译技术：使得纯 IPv6 结点与纯 IPv4 结点之间可以进行通信。

参考答案

（27）B （28）D

试题（29）

原站收到“在数据包组装期间生存时间为 0”的 ICMP 报文，出现的原因是__（29）__。

（29）A．IP 数据报目的地址不可达 B．IP 数据报目的网络不可达

C．ICMP 报文校验差错 D．IP 数据报分片丢失

试题（29）分析

本题考查 ICMP 报文及使用情况相关基础知识。

在 IP 报文传输过程中出现错误或对对方主机进行探测时发送 ICMP 报文。ICMP 报文报告的差错有多种，其中源站收到“在数据包组装期间生存时间为 0”的 ICMP 报文时，说明 IP 数据报分片丢失。IP 报文在经历 MTU 较小的网络时，会进行分片和重装，在重装路由器上对同一分组的所有分片报文维持一个计时器，当计时器超时还有分片没到，重装路由器会丢弃收到的该分组的所有分片，并向源站发送“在数据包组装期间生存时间为 0”的 ICMP 报文。

参考答案

（29）D

试题（30）

下列 DHCP 报文中，由客户端发送给 DHCP 服务器的是__（30）__。

（30）A．DhcpOffer B．DhcpDecline

C．DhcpAck D．DhcpNack

试题（30）分析

本题考查 DHCP 报文相关基础知识。

DhcpOffer 是服务器在收到客户端发现报文，且可为其分配 IP 地址时发送的响应报文；DhcpAck 是服务器端在接收到客户端请求报文后，为客户端分配地址时采用的报文；DhcpAck 是服务器端在接收到客户端请求报文后，不能为客户端分配地址时采用的报文；

如果客户端发现 DHCP SERVER 分配的 IP 地址已经被别人使用，会发出 DhcpDecline 报文通知 DHCP SERVER 禁用这个 IP 地址，以免引起 IP 地址冲突。

参考答案

（30）B

试题（31）

在 Windows 用户管理中，使用组策略 A-G-DL-P，其中 DL 表示<u>（31）</u>。

（31）A．用户账号　　B．资源访问权限
C．域本地组　　D．通用组

试题（31）分析

本题考查 Windows 用户组策略相关基础知识。

组策略 A-G-DL-P 中，A 是用户账号，G 表示全局组，DL 表示域本地组，P 表示资源访问权限。

参考答案

（31）C

试题（32）

在光纤测试过程中，存在强反射时，使得光电二极管饱和，光电二极管需要一定的时间由饱和状态中恢复，在这一时间内，它将不会精确地检测后散射信号，在这一过程中没有被确定的光纤长度称为盲区。盲区一般表现为前端盲区，为了解决这一问题，可以<u>（32）</u>，以便将此效应减到最小。

（32）A．采用光功率计进行测试
B．在测试光缆后加一条长的测试光纤
C．在测试光缆前加一条长的测试光纤
D．采用 OTDR 进行测试

试题（32）分析

本题考查光纤测试实际工程项目知识。

在测试光缆前加一条长的测试光纤来解决前端盲区问题。

参考答案

（32）C

试题（33）、（34）

S/MIME 发送报文的过程中对消息 M 的处理包括生成数字指纹、生成数字签名、加密数字签名和加密报文 4 个步骤，其中生成数字指纹采用的算法是<u>（33）</u>，加密数字签名采用的算法是<u>（34）</u>。

（33）A．MD5　　B．3DES　　C．RSA　　D．RC2

（34）A．MD5　　B．RSA　　C．3DES　　D．SHA-1

试题（33）、（34）分析

本题考查安全协议 S/MIME 对报文的处理过程。

S/MIME 发送报文的过程中，对消息 M 的处理包括生成数字指纹、生成数字签名、加密数字签名和加密报文 4 个步骤。首先生成的数字指纹是对消息采用 Hash 运算之后的摘要，四个选项中只有 MD5 是摘要算法；生成数字签名通常采用公钥算法；加密数字签名需采用对称密钥，四个选项中只有 3DES 是对称密钥；加密报文也得采用对称密钥，计算复杂性较小。

参考答案

（33）A　（34）C

试题（35）、（36）

下列 DNS 查询过程中，采用迭代查询的是__（35）__，采用递归查询的是__（36）__。

（35）A．客户端向本地 DNS 服务器发出查询请求
B．客户端在本地缓存中找到目标主机的地址
C．本地域名服务器把查询请求发送给转发器
D．由根域名服务器找到授权域名服务器的地址

（36）A．转发器查询非授权域名服务器
B．客户端向本地域名服务器发出查询请求
C．由上级域名服务器给出下级域名服务器的地址
D．由根域名服务器找到授权域名服务器的地址

试题（35）、（36）分析

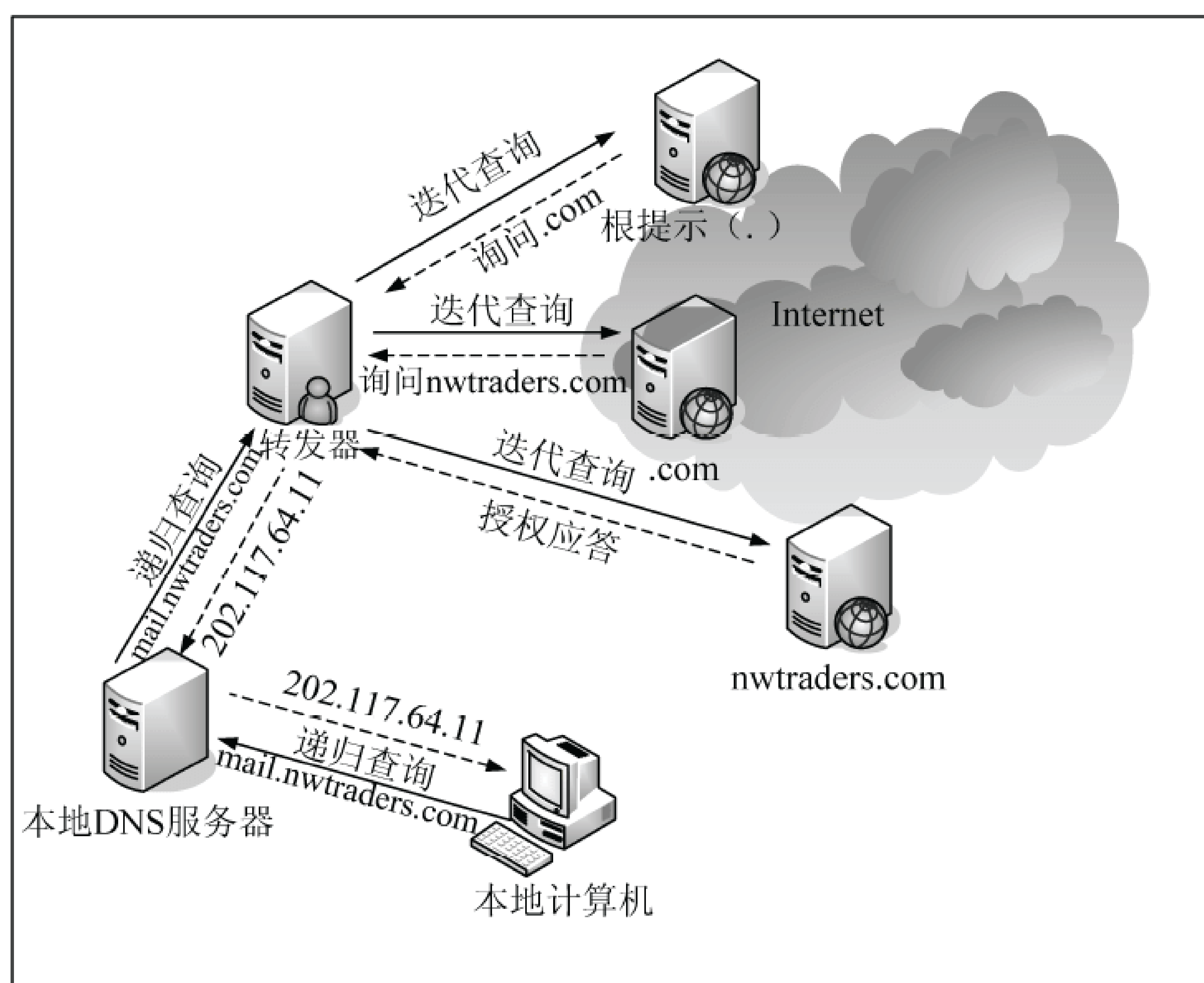
DNS 查询过程分为两种查询方式：

① 递归查询：当用户发出查询请求时，本地服务器要进行递归查询。这种查询方式要求服务器彻底地进行名字解析，并返回最后的结果——IP 地址或错误信息。如果查询请求在本地服务器中不能完成，那么服务器就根据它的配置向域名树中的上级服务器进行查询，在最坏的情况下可能要查询到根服务器。每次查询返回的结果如果是其他名字服务器的 IP 地址，则本地服务器要把查询请求发送给这些服务器做进一步的查询。

② 迭代查询：服务器与服务器之间的查询采用迭代的方式进行，发出查询请求的服务器得到的响应可能不是目标的 IP 地址，而是其他服务器的引用（名字和地址），那么本地服务器就要访问被引用的服务器，做进一步的查询。如此反复多次，每次都更接近目标的授权服务器，直至得到最后的结果——目标的 IP 地址或错误信息。

关于递归查询和迭代查询应用的具体场合可参见下图，首先是本地计算机向本地 DNS 服务器进行递归查询，本地服务器查找不到需要的记录，则向转发器发出递归查询

请求。转发器通过迭代查询得到需要的结果后，转发给本地 DNS 服务器，并返回本地计算机。



参考答案

（35）D　（36）B

试题（37）

DHCP 服务器分配的默认网关地址是 220.115.5.33/28，__（37）__是该子网的主机地址。

（37）A．220.115.5.32　　B．220.115.5.40

C．220.115.5.47　　D．220.115.5.55

试题（37）分析

由于默认网关的地址为 220.115.5.33/28，所以与其同一子网的主机地址为 220.115.5.40，参见下面的二进制表示。

220.115.5.33/28：　**1101 1100.0111 0011.0000 0101.0010** 0001

220.115.5.40：　**1101 1100.0111 0011.0000 0101.0010** 1000

参考答案

（37）B

试题（38）

主机地址 122.34.2.160 属于子网__（38）__。

（38）A．122.34.2.64/26　　B．122.34.2.96/26

C．122.34.2.128/26　　D．122.34.2.192/26

试题（38）分析

主机地址 122.34.2.160 的二进制表示为： 0111 1010.0010 0010.0000 0010.1010 0000

与其匹配的子网地址为 122.34.2.128/26： **0111 1010.0010 0010.0000 0010.10**00 0000

参考答案

（38）C

试题（39）

某公司的网络地址为 192.168.1.0，要划分成 5 个子网，每个子网最多 20 台主机，则适用的子网掩码是__（39）__。

（39）A．255.255.255.192　　B．255.255.255.240

C．255.255.255.224　　D．255.255.255.248

试题（39）分析

子网掩码应为 255.255.255.224，其二进制表示为：

1111 1111.1111 1111.1111 1111.1110 0000

最后 3 个 1 用来区分 5 个子网，最右边的 5 位可提供最多 30 个主机地址。

参考答案

（39）C

试题（40）

以下关于 IPv6 的论述中，正确的是__（40）__。

（40）A．IPv6 数据包的首部比 IPv4 复杂

B．IPv6 的地址分为单播、广播和任意播 3 种

C．IPv6 地址长度为 128 比特

D．每个主机拥有唯一的 IPv6 地址

试题（40）分析

IPv6 地址增加到 128 位，并且能够支持多级地址层次；地址自动配置功能简化了网络地址的管理；在组播地址中增加了范围字段，改进了组播路由的可伸缩性；增加的任意播地址比 IPv4 中的广播地址更加实用。

IPv6 地址是一个或一组接口的标识符。IPv6 地址被分配到接口，而不是分配给结点。IPv6 地址有 3 种类型：

① 单播（Unicast）地址

② 任意播（AnyCast）地址

③ 组播（MultiCast）地址

在 IPv6 地址中，任何全“0”和全“1”字段都是合法的，除非特别排除的之外。特别是前缀可以包含“0”值字段，也可以用“0”作为终结字段。一个接口可以被赋予任何类型的多个地址（单播、任意播、组播）或地址范围。

与 IPv4 相比，IPv6 首部有下列改进：

① 分组头格式得到简化：IPv4 头中的很多字段被丢弃，IPv6 头中字段的数量从 12 个降到了 8 个，中间路由器必须处理的字段从 6 个降到了 4 个，这样就简化了路由器的处理过程，提高了路由选择的效率。

② 改进了对分组头部选项的支持：与 IPv4 不同，路由选项不再集成在分组头中，而是把扩展头作为任选项处理，仅在需要时才插入到 IPv6 头与负载之间。这种方式使得分组头的处理更灵活，也更流畅。以后如果需要，还可以很方便地定义新的扩展功能。

③ 提供了流标记能力：IPv6 增加了流标记，可以按照发送端的要求对某些分组进行特别的处理，从而提供了特别的服务质量支持，简化了对多媒体信息的处理，可以更好地传送具有实时需求的应用数据。

参考答案

（40）C

试题（41）、（42）

按照 RSA 算法，取两个大素数 p 和 q，$n=p\times q$，令 $\varphi(n)=(p-1)\times(q-1)$，取与 $\varphi(n)$ 互质的数 e，$d=e^{-1} \bmod \varphi(n)$，如果用 M 表示消息，用 C 表示密文，下面 （41） 是加密过程， （42） 是解密过程。

（41）A．$C=M^e \bmod n$　　B．$C=M^n \bmod d$

C．$C=M^d \bmod \varphi(n)$　　D．$C=M^n \bmod \varphi(n)$

（42）A．$M=C^n \bmod e$　　B．$M=C^d \bmod n$

C．$M=C^d \bmod \varphi(n)$　　D．$M=C^n \bmod \varphi(n)$

试题（41）、（42）分析

本题考查 RSA 算法的基础知识。

RSA（Rivest Shamir and Adleman）是一种公钥加密算法。方法是按照下面的要求选择公钥和密钥。

1．选择两个大素数 p 和 q（大于 10^{100}）。

2．令 $n=p\times q$ 和 $z=(p-1)\times(q-1)$。

3．选择 d 与 z 互质。

4．选择 e，使 $e\times d=1 \pmod z$。

明文 P 被分成 k 位的块，k 是满足 $2^k<n$ 的最大整数，于是有 $0\leqslant P<n$。加密时计算

$C=P^e \pmod n$

这样公钥为（e,n）。解密时计算

$P=C^d \pmod n$

即私钥为（d,n）。

参考答案

（41）A　（42）B

试题（43）

A 和 B 分别从 CA_1 和 CA_2 两个认证中心获取了自己的证书 I_A 和 I_B，要使 A 能够对 B 进行认证，还需要__（43）__。

（43）A．A 和 B 交换各自公钥　　B．A 和 B 交换各自私钥

C．CA_1 和 CA_2 交换各自公钥　　D．CA_1 和 CA_2 交换各自私钥

试题（43）分析

本题考查 CA 数字证书认证的基础知识。

CA 为用户产生的证书应具有以下特性。

① 只要得到 CA 的公钥，就能由此得到 CA 为用户签署的公钥。

② 除 CA 外，其他任何人员都不能以不被察觉的方式修改证书的内容。

如果所有用户都由同一 CA 签署证书，则这一 CA 就必须取得所有用户的信任。如果用户数量很多，仅一个 CA 负责为所有用户签署证书就可能不现实。通常应有多个 CA，每个 CA 为一部分用户发行和签署证书。用户之间需要进行认证，首先需要对各自的认证中心进行认证，要认证 CA，则需 CA 和 CA 之间交换各自的证书。

参考答案

（43）C

试题（44）

如图所示，①，②和③是三种数据包的封装方式，以下关于 IPSec 认证头方式中，所使用的封装与其所对应模式的匹配，__（44）__是正确的。

①	原IP头	TCP	DATA		
②	原IP头	AH	TCP	DATA	
③	新IP头	AH	原IP头	TCP	DATA

（44）A．传输模式采用封装方式①　　B．隧道模式采用封装方式②

C．隧道模式采用封装方式③　　D．传输模式采用封装方式③

试题（44）分析

本题考查 IPSec 数据封装的基础知识。

IPSec 传送认证或加密的数据之前，必须就协议、加密算法和使用的密钥进行协商。密钥交换协议提供这个功能，并且在密钥交换之前还要对远程系统进行初始的认证。

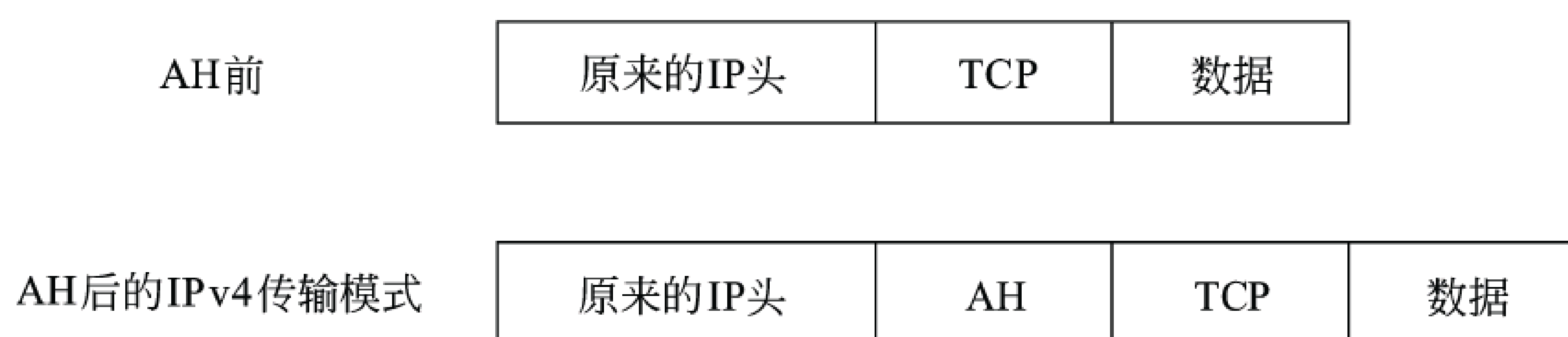
IPSec 认证头提供了数据完整性和数据源认证，但是不提供保密服务。AH 包含了对称密钥的散列函数，使得第三方无法修改传输中的数据。IPSec 支持下面的认证算法。

① HMAC-SHA1（Hashed Message Authentication Code-Secure Hash Algorithm 1），128 位密钥。

② HMAC-MD5（HMAC-Message Digest 5），160 位密钥。

IPSec 有两种模式：传输模式和隧道模式。在传输模式中，IPSec 认证头插入原来的

IP 头之后（如下图所示），IP 数据和 IP 头用来计算 AH 认证值。IP 头中的变化字段（例如跳步计数和 TTL 字段）在计算之前置为 0，所以变化字段实际上并没有被认证。



传输模式的认证头

在隧道模式中，IPSec 用新的 IP 头封装了原来的 IP 数据报（包括原来的 IP 头），原来 IP 数据报的所有字段都经过了认证，如下图所示。



隧道模式的认证头

参考答案

（44）C

试题（45）

下列协议中，不用于数据加密的是__（45）__。

（45）A. IDEA　　B. Differ-hellman　　C. AES　　D. RC4

试题（45）分析

本题考查加密算法基础知识。

现代密码体制使用的基本方法仍然是替换和换位，但是采用更加复杂的加密算法和简单的密钥，而且增加了对付主动攻击的手段，例如加入随机的冗余信息，以防止制造假消息；加入时间控制信息，以防止旧消息重放。

常见的加密算法有 DES（Data Encryption Standard）加密算法、三重 DES（Triple-DES）加密算法、IDEA（International Data Encryption Algorithm）加密算法、高级加密标准（Advanced Encryption Standard，AES）加密算法、流加密算法和 RC4。

Diffie-Hellman 是一种确保共享 KEY 安全穿越不安全网络的方法，它是由 Whitefield 与 Martin Hellman 在 1976 年提出的一种奇妙的密钥交换协议，称为 Diffie-Hellman 密钥交换协议/算法（Diffie-Hellman Key Exchange/Agreement Algorithm）。这个机制的巧妙在于需要安全通信的双方可以用这个方法确定对称密钥。然后可以用这个密钥进行加密和解密。但是注意，这个密钥交换协议/算法只能用于密钥的交换，而不能进行消息的加密和解密。双方确定要用的密钥后，要使用其他对称密钥操作加密算法实际加密和解密

消息。

参考答案

（45）B

试题（46）

下列关于数字证书的说法中，正确的是__（46）__。

（46）A．数字证书是在网上进行信息交换和商务活动的身份证明
B．数字证书使用公钥体制，用户使用公钥进行加密和签名
C．在用户端，只需维护当前有效的证书列表
D．数字证书用于身份证明，不可公开

试题（46）分析

本题考查数字证书的基础知识。

数字证书是各类终端实体和最终用户在网上进行信息交流及商务活动的身份证明，在电子交易的各个环节，交易的各方都需验证对方数字证书的有效性，从而解决相互间的信任问题。

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密和解密。每个用户自己设定一个特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名，同时设定一个公共密钥（公钥），并由本人公开，为一组用户所共享，用于加密和验证。公开密钥技术解决了密钥发布的管理问题。一般情况下，证书中还包括密钥的有效时间、发证机构（证书授权中心）的名称及该证书的序列号等信息。数字证书的格式遵循 ITUT X.509 国际标准。

参考答案

（46）A

试题（47）

PPP 协议不包含__（47）__。

（47）A．封装协议　　B．点对点隧道协议（PPTP）
C．链路控制协议（LCP）　　D．网络控制协议（NCP）

试题（47）分析

本题考查 PPP 协议的基础知识。

PPP 协议（Point-to-Point Protocol）可以在点对点链路上传输多种上层协议的数据包。PPP 是数据链路层协议，最早是替代 SLIP 协议用来在同步链路上封装 IP 数据报的，后来也可以承载诸如 DECnet、Novell IPX、Apple Talk 等协议的分组。PPP 是一组协议，包含下列成分。

① 封装协议。用于包装各种上层协议的数据报。PPP 封装协议提供了在同一链路上传输各种网络层协议的多路复用功能，也能与各种常见的支持硬件保持兼容。

② 链路控制协议（Link Control Protocol，LCP）。通过以下三类 LCP 分组来建立、

配置和管理数据链路连接。

③ 网络控制协议。在 PPP 的链路建立过程中的最后阶段将选择承载的网络层协议，例如 IP、IPX 或 AppleTalk 等。PPP 只传送选定的网络层分组，任何没有入选的网络层分组将被丢弃。

参考答案

（47）B

试题（48）

以下关于数据备份策略的说法中，错误的是__（48）__。

（48）A．完全备份是备份系统中所有的数据

B．增量备份是只备份上一次完全备份后有变化的数据

C．差分备份是指备份上一次完全备份后有变化的数据

D．完全、增量和差分三种备份方式通常结合使用，以发挥出最佳的效果

试题（48）分析

本题考查数据备份策略的基础知识。

完全备份就是备份系统中所有的数据，并不依赖文件的存档属性来确定备份哪些文件。在备份过程中，任何现有的标记都被清除，每个文件都被标记为已备份。换言之，清除存档属性。差分备份仅对自上一次完全备份之后有变化的数据进行备份。差分备份过程中，只备份有标记的那些选中的文件和文件夹。它不清除标记，也即备份后不标记为已备份文件。换言之，不清除存档属性。增量备份自上一次备份（包含完全备份、差分备份、增量备份）之后有变化的数据。增量备份过程中，只备份有标记的选中的文件和文件夹，它清除标记，即备份后标记文件，换言之，清除存档属性。完全、增量和差分三种备份方式通常结合使用，以发挥出最佳的效果。

参考答案

（48）B

试题（49）、（50）

假如有 3 块容量是 80G 的硬盘做 RAID 5 阵列，则这个 RAID 5 的容量是__（49）__；而如果有 2 块 80G 的盘和 1 块 40G 的盘，此时 RAID 5 的容量是__（50）__。

（49）A．240G　B．160G　C．80G　D．40G

（50）A．40G　B．80G　C．160G　D．200G

试题（49）、（50）分析

本题考查 RAID 的基础概念。

RAID（Redundant Array of Independent Disks）的中文简称为独立冗余磁盘阵列。简单的说，RAID 是一种把多块独立的硬盘（物理硬盘）按不同的方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能和提供数据备份技术。组成磁盘阵列的不同方式称为 RAID 级别（RAID Levels）。在用户看起来，组成的磁盘组就

像是一个硬盘，用户可以对它进行分区，格式化等。总之，对磁盘阵列的操作与单个硬盘一模一样。不同的是，磁盘阵列的存储速度要比单个硬盘高很多，而且可以提供自动数据备份。数据备份的功能是在用户数据一旦发生损坏后，利用备份信息可以使损坏数据得以恢复，从而保障了用户数据的安全性。RAID 技术分为几种不同的等级，分别可以提供不同的速度，安全性和性价比。根据实际情况选择适当的 RAID 级别可以满足用户对存储系统可用性、性能和容量的要求。常用的 RAID 级别有以下几种：NRAID，JBOD，RAID0，RAID1，RAID1+0，RAID3，RAID5 等。目前经常使用的是 RAID5 和 RAID（1+0）。如果使用物理硬盘容量不相等的硬盘做 RAID，那么创建的 RAID 阵列的总容量为较小的硬盘的计算方式。

RAID5 的存储机制是两块存数据，一块存另外两块硬盘的交易校验结果。RAID5 建立后，坏掉一块硬盘，可以通过另外两块硬盘的数据算出第三块的，所以至少要 3 块。RAID5 是一种旋转奇偶校验独立存取的阵列方式，它与 RAID3、RAID4 不同的是没有固定的校验盘，而是按某种规则把奇偶校验信息均匀地分布在阵列所属的硬盘上，所以在每块硬盘上，既有数据信息也有校验信息。这一改变解决了争用校验盘的问题，使得在同一组内并发进行多个写操作。所以 RAID5 既适用于大数据量的操作，也适用于各种事务处理，它是一种快速、大容量和容错分布合理的磁盘阵列。当有 N 块阵列盘时，用户空间为 N-1 块盘容量。

根据以上原理，共有 3 块 80G 的硬盘做 RAID 5，则总容量为（3-1）×80=160G；如果有 2 块 80G 的盘和 1 块 40G 的盘，则以较小的盘的容量为计算方式，总容量为（3-1）×40=80G。

参考答案

（49）B　　　（50）B

试题（51）

以下关于网络分层模型的叙述中，正确的是＿（51）＿。

（51）A. 核心层为了保障安全性，应该对分组进行尽可能多的处理
　　　B. 汇聚层实现数据分组从一个区域到另一个区域的高速转发
　　　C. 过多的层次会增加网络延迟，并且不便于故障排查
　　　D. 接入层应提供多条路径来缓解通信瓶颈

试题（51）分析

本题考查网络需求分析中分层模型的各层功能。

核心层的目的是保障高速转发，需要对分组进行尽可能少的处理；汇聚层实现由接入层传递数据的汇聚，实现包过滤等安全处理；接入层负责用户的接入，无须冗余路径。的确，过多的层次会增加网络延迟，并且不便于故障排查。

参考答案

（51）C

试题（52）

以下关于网络规划设计过程的叙述中，属于需求分析阶段任务的是__（52）__。

（52）A．依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B．制定对设备厂商、服务提供商的选择策略

C．根据需求规范和通信规范，实施资源分配和安全规划

D．确定网络设计或改造的任务，明确新网络的建设目标

试题（52）分析

本题考查网络需求分析中各阶段的功能。

依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境是物理设计阶段的任务；制定对设备厂商、服务提供商的选择策略是逻辑设计阶段的任务；根据需求规范和通信规范，实施资源分配和安全规划是逻辑设计阶段的任务；确定网络设计或改造的任务，明确新网络的建设目标是需求阶段的任务。

参考答案

（52）D

试题（53）、（54）

某高校欲构建财务系统，使得用户可通过校园网访问该系统。根据需求，公司给出如下 2 套方案：

方案一：

（1）出口设备采用一台配置防火墙板卡的核心交换机，并且使用防火墙策略将需要对校园网做应用的服务器进行地址映射；

（2）采用 4 台高性能服务器实现整体架构，其中 3 台作为财务应用服务器，1 台作为数据备份管理服务器；

（3）通过备份管理软件的备份策略将 3 台财务应用服务器的数据进行定期的备份。

方案二：

（1）出口设备采用一台配置防火墙板卡的核心交换机，并且使用防火墙策略将需要对校园网做应用的服务器进行地址映射；

（2）采用 2 台高性能服务器实现整体架构，服务器采用虚拟化技术，建多个虚拟机满足财务系统业务需求。当一台服务器出现物理故障时将业务迁移到另外一台物理服务器上。

与方案一相比，方案二的优点是__（53）__。方案二还有一些缺点，下列不属于其缺点的是__（54）__。

（53）A．网络的安全性得到保障　　B．数据的安全性得到保障

C．业务的连续性得到保障　　D．业务的可用性得到保障

（54）A．缺少企业级磁盘阵列，不能将数据进行统一的存储与管理

B．缺少网闸，不能实现财务系统与 Internet 的物理隔离

C．缺少安全审计，不便于相关行为的记录、存储与分析

D．缺少内部财务用户接口，不便于快速管理与维护

试题（53）、（54）分析

本题考查网络规划与设计案例。

与方案一相比，方案二服务器采用虚拟化技术，当一台服务器出现物理故障时将业务迁移到另外一台物理服务器上，保障了业务的连续性。网络的安全性、数据的安全性、业务的可用性都没有发生实质性变化。

当然方案二还有一些缺陷，首先是缺少将数据进行统一的存储与管理的企业级磁盘阵列；其次缺少安全审计，不便于相关行为的记录、存储与分析；而且缺少内部财务用户接口，不便于快速管理与维护。但是如果加网闸，就不能实现对财务系统的访问。不能实现用户可通过校园网对财务系统的访问。

参考答案

（53）C （54）B

试题（55）～（57）

某大学拟建设无线校园网，委托甲公司承建。甲公司的张工带队去进行需求调研，获得的主要信息有：

校园面积约 $4km^2$，要求室外绝大部分区域及主要建筑物内实现覆盖，允许同时上网用户数量为 5000 以上，非本校师生不允许自由接入，主要业务类型为上网浏览、电子邮件、FTP、QQ 等，后端与现有校园网相连。

张工据此撰写了需求分析报告，提交了逻辑网络设计方案，其核心内容包括：

① 网络拓扑设计

② 无线网络设计

③ 安全接入方案设计

④ 地址分配方案设计

⑤ 应用功能配置方案设计

以下三个方案中，符合学校要求、合理可行的是：

无线网络选型的方案采用__（55）__；

室外供电的方案是__（56）__；

无线网络安全接入的方案是__（57）__。

（55）A．基于 WLAN 的技术建设无线校园网

B．基于固定 WiMAX 的技术建设无线校园网

C．直接利用电信运营商的 3G 系统

D．暂缓执行，等待移动 WiMAX 成熟并商用

（56）A．采用太阳能供电　　B．地下埋设专用供电电缆

C．高空架设专用供电电缆　　D．以 PoE 方式供电

（57）A．通过 MAC 地址认证　　B．通过 IP 地址认证
　　C．通过用户名与密码认证　　D．通过用户的物理位置认证

试题（55）～（57）分析

本题考查网络规划与设计案例。

首先，无线网络选型时基于 WLAN 的技术建设无线校园网是经济可行的方案；其次室外供电的方案是以 PoE 方式供电，太阳能供电不能保障不间断，地下埋设专用供电电缆以及高空架设专用供电电缆覆盖的范围较大，工程复杂。无线网络安全接入的方案是通过用户名与密码认证，其他方式都不适用。

参考答案

（55）A　　（56）D　　（57）C

试题（58）

互联网上的各种应用对网络 QoS 指标的要求不一，下列应用中对实时性要求最高的是__（58）__。

（58）A．浏览页面　　B．视频会议
　　C．邮件接收　　D．文件传输

试题（58）分析

本题考查网络应用及 QoS。

浏览页面、邮件接收以及文件传输对实时性没有太高要求，视频会议必须保障实时性。

参考答案

（58）B

试题（59）

下列关于网络测试的说法中，正确的是__（59）__。

（59）A．接入-汇聚链路测试的抽样比例应不低于 10%
　　B．当汇聚-核心链路数量少于 10 条时，无须测试网络传输速率
　　C．丢包率是指网络空载情况下，无法转发数据包的比例
　　D．连通性测试要求达到 5 个 9 标准，即 99.999%

试题（59）分析

本题考查网络测试的基础知识。

网络系统测试主要是测试网络是否为应用系统提供了稳定、高效的网络平台，如果网络系统不够稳定，网络应用就不可能快速稳定。对常规的以太网进行系统测试，主要包括系统连通性、链路传输速率、吞吐率、传输时延及链路层健康状况测试等基本功能测试。

所有联网的终端都必须按使用要求全部连通。

连通性测试方法一般有：

① 将测试工具连接到选定的接入层设备的端口，即测试点。

② 用测试工具对网络的关键服务器、核心层和汇聚层的关键网络设备（如交换机和路由器），进行 10 次 Ping 测试，每次间隔 1s，以测试网络连通性。测试路径要覆盖所有的子网和 VLAN。

③ 移动测试工具到其他位置测试点，重复步骤②，直到遍历所有测试抽样设备。

抽样规则以不低于接入层设备总数 10%的比例进行抽样测试，抽样少于 10 台设备的，全部测试；每台抽样设备中至少选择一个端口，即测试点应能够覆盖不同的子网和 VLAN。

合格标准分为单项合格判据和综合合格判据两种。

单项合格判据：测试点到关键节点的 Ping 测试连通性达到 100%时，则判定单点连通性符合要求。

综合合格判据：所有测试点的连通性都达到 100%时，则判定系统的连通性符合要求；否则判定系统的连通性不符合要求。

参考答案

（59）A

试题（60）

网络测试技术有主动测试和被动测试两种方式， （60） 是主动测试。

（60）A．使用 Sniffer 软件抓包并分析　　B．向网络中发送大容量 ping 报文
　　　C．读取 SNMP 的 MIB 信息并分析　　D．查看当前网络流量状况并分析

试题（60）分析

本题考查网络测试的基础知识。

网络测试有多种方法，根据测试中是否向被测网络注入测试流量，可以将网络测试方法分为主动测试和被动测试。

主动测试是指利用测试工具有目的地主动向被测网络注入测试流量，并根据这些测试流量的传送情况来分析网络技术参数的测试方法。主动测试具备良好的灵活性，它能够根据测试环境明确控制测量中所产生的测量流量的特征，如特性、采样技术、时标频率、调度、包大小、类型（模拟各种应用）等，主动测试使测试能够按照测试者的意图进行，容易进行场景仿真。主动测试的问题在于安全性。由于主动测试主动向被测网络注入测试流量，是“入侵式”的测量，必然会带来一定的安全隐患。如果在测试中进行细致的测试规划，可以降低主动测试的安全隐患。

被动测试是指利用特定测试工具收集网络中活动的元素（包括路由器、交换机、服务器等设备）的特定信息，以这些信息作为参考，通过量化分析，实现对网络性能、功能进行测量的方法。常用的被动测试方式包括：通过 SNMP 协议读取相关 MIB 信息，通过 Sniffer、Ethereal 等专用数据包捕获分析工具进行测试。被动测试的优点是它的安全性。被动测试不会主动向被测网络注入测试流量，因此就不会存在注入 DDoS、网络

欺骗等安全隐患；被动测试的缺点是不够灵活，局限性较大，而且因为是被动地收集信息，并不能按照测量者的意愿进行测试，会受到网络机构、测试工具等多方面的限制。

参考答案

（60）B

试题（61）

以下关于网络故障排除的说法中，错误的是__（61）__。

（61）A．ping 命令支持 IP、AppleTalk、Novell 等多种协议中测试网络的连通性

B．可随时使用 debug 命令在网络设备中进行故障定位

C．tracert 命令用于追踪数据包传输路径，并定位故障

D．show 命令用于显示当前设备或协议的工作状况

试题（61）分析

本题考查网络故障排除的基础知识。

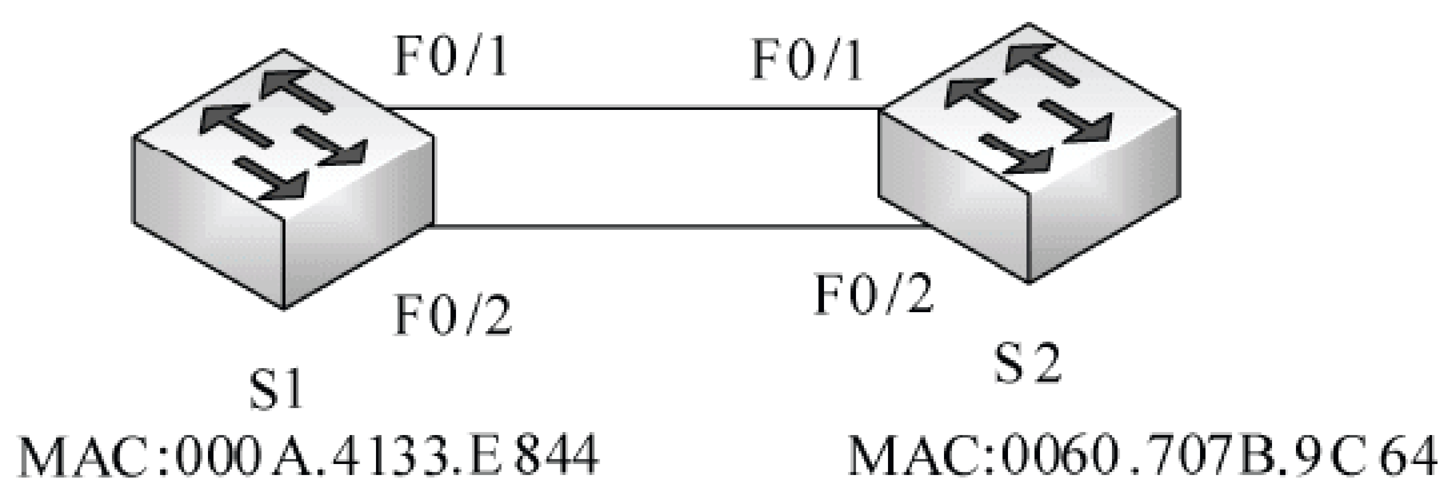
debug 命令是用于在网络中进行故障排查和故障定位的命令，该命令运行时，需耗费网络设备相当大的 CPU 资源，且会持续较长的时间，通常会造成网络效率的严重降低，甚至不可用。基于此，当需要使用 debug 命令来排查网络中的故障时，通常需在网络压力较小的时候进行，例如凌晨 2:00～6:00 这个时间段。

参考答案

（61）B

试题（62）

如图所示，交换机 S1 和 S2 均为默认配置，使用两条双绞线连接，__（62）__接口的状态是阻塞状态。



（62）A．S1 的 F0/1　　B．S2 的 F0/1　　C．S1 的 F0/2　　D．S2 的 F0/2

试题（62）分析

本题考查生成树协议的基础知识。

当两台交换机之间存在冗余链路时，势必会造成环路，为避免该情况的发生，交换机中自动开启的生成树协议会根据一定的选举规则将其中一个端口的状态调整为阻塞状态，以断开环路连接，以免造成网络风暴。选举规则是：首先确定根桥，优先级较高的交换机会被选举为根桥，优先级默认情况下相同，当优先级相同时，交换机 MAC 地址较小者会被选举为根桥，根桥上的端口均为根端口，根端口不会被设置为阻塞状态，非

根桥交换机上的端口优先级较高（值小）者为指定端口，较低者为非指定端口（阻塞端口），当接口优先级相同时，则比较接口编号，接口编号较大者将会被置为阻塞状态。

参考答案

（62）D

试题（63）

以下关于网络布线子系统的说法中，错误的是__（63）__。

（63）A. 工作区子系统指终端到信息插座的区域

B. 水平子系统是楼层接线间配线架到信息插座，线缆最长可达 100m

C. 干线子系统用于连接楼层之间的设备间，一般使用数对大铜缆或光纤布线

D. 建筑群子系统连接建筑物，布线可采取地下管道铺设、直埋或架空明线

试题（63）分析

本题考查综合布线的基础知识。

在综合布线系统中，分为工作区子系统、水平子系统、垂直干线子系统、管理子系统、建筑群子系统和设备间子系统。

工作区子系统的目的是实现工作区终端设备与水平子系统之间的连接，由终端设备连接到信息插座的连接线缆所组成。

水平子系统的目的是实现信息插座和管理子系统（跳线架）间的连接，将用户工作区引至管理子系统，并为用户提供一个符合国际标准，满足语音及高速数据传输要求的信息点出口，当使用双绞线为传输介质时，其最大传输距离为 100 米，而水平子系统连接着工作区与其他子系统，需为工作区子系统预留有一定长度的线缆余量，因此水平子系统的电缆长度一般不应超过 100 米。

垂直干线子系统的目的是实现计算机设备、程控交换机（PBX）、控制中心与各管理子系统间的连接，是建筑物干线电缆的路由。

管理子系统由交连、互连配线架组成。管理点为连接其他子系统提供连接手段。交连和互连允许将通讯线路定位或重定位到建筑物的不同部分，以便能更容易地管理通信线路，使在移动终端设备时能方便地进行插拔。

建筑群子系统将一个建筑物的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置上，是结构化布线系统的一部分，支持提供楼群之间通信所需的硬件。

设备间子系统主要是由设备间中的电缆、连接器和有关的支撑硬件组成，作用是将计算机、PBX、摄像头、监视器等弱电设备互连起来并连接到主配线架上。

参考答案

（63）B

试题（64）

某学生宿舍采用 ADSL 接入 Internet，为扩展网络接口，用双绞线将两台家用路由器连接在一起，出现无法访问 Internet 的情况，导致该问题最可能的原因是__（64）__。

（64）A．双绞线质量太差　　B．两台路由器上的 IP 地址冲突
C．有强烈的无线信号干扰　　D．双绞线类型错误

试题（64）分析

本题考查网络故障排查的基本知识。

通常，目前市面上出售的家用路由器在默认情况下具备 DHCP、NAPT、扩展网络接口、简单的流量控制等功能。根据题目说明，使用 ADSL 接入 Internet，家用路由器应该采用的是动态 IP 地址的设置，如将两台家用路由器简单地使用双绞线相连时，两台路由器会将彼此认为是客户端，其上默认打开的 DHCP 服务器均会为对方分配 IP 地址，这样就会造成 IP 地址冲突，而导致无法通信。

参考答案

（64）B

试题（65）

IP SAN 区别于 FC SAN 以及 IB SAN 的主要技术是采用__（65）__实现异地间的数据交换。

（65）A．I/O　　B．iSCSI
C．InfiniBand　　D．Fibre Channel

试题（65）分析

本题考查网络应用及 QoS。

IP SAN 区别于 FC SAN 以及 IB SAN 的主要技术是采用 iSCSI 实现异地间的数据交换，IB SAN 的主要技术是采用 InfiniBand。

参考答案

（65）B

试题（66）

如果本地域名服务器无缓存，当采用递归法解析另一个网络的某主机域名时，用户主机、本地域名服务器发送的域名请求消息数分别为__（66）__。

（66）A．一条，一条　　B．一条，多条
C．多条，一条　　D．多条，多条

试题（66）分析

本题考查域名解析中递归法解析的基础知识。

递归查询是最常见的查询方式，域名服务器将代替提出请求的客户机（下级 DNS 服务器）进行域名查询，若域名服务器不能直接回答，则域名服务器会在域名树中的各分支的上下进行递归查询，最终将查询结果返回给客户机。在域名服务器查询期间，客户机将完全处于等待状态。如果本地域名服务器无缓存，当采用递归法解析另一个网络的某主机域名时，用户主机发送的域名请求消息数为一条，这时本地域名服务器发送的域名请求消息数也为一条。

参考答案

（66）A

试题（67）

由于 OSI 各层功能具有相对性，在网络故障检测时按层排查故障可以有效发现和隔离故障，通常逐层分析和排查的策略在具体实施时__（67）__。

（67）A．从低层开始　　B．从高层开始
C．从中间开始　　D．根据具体情况选择

试题（67）分析

本题考查网络故障检测的基础知识。

在网络故障检测时按 OSI 模型的各层排查故障可以有效发现和隔离故障，通常逐层分析和排查的策略在具体实施时要根据具体情况来判断。因为通常故障的表现可以让我们选择具体的故障到底是在物理层、数据链路层或者网络层等，这样就可以省时省力快速判断并解决问题。

参考答案

（67）D

试题（68）

在网络故障检测中，将多个子网断开后分别作为独立的网络进行测试，属于__（68）__检查。

（68）A．整体　　B．分层　　C．分段　　D．隔离

试题（68）分析

本题考查网络故障检测的基础知识。

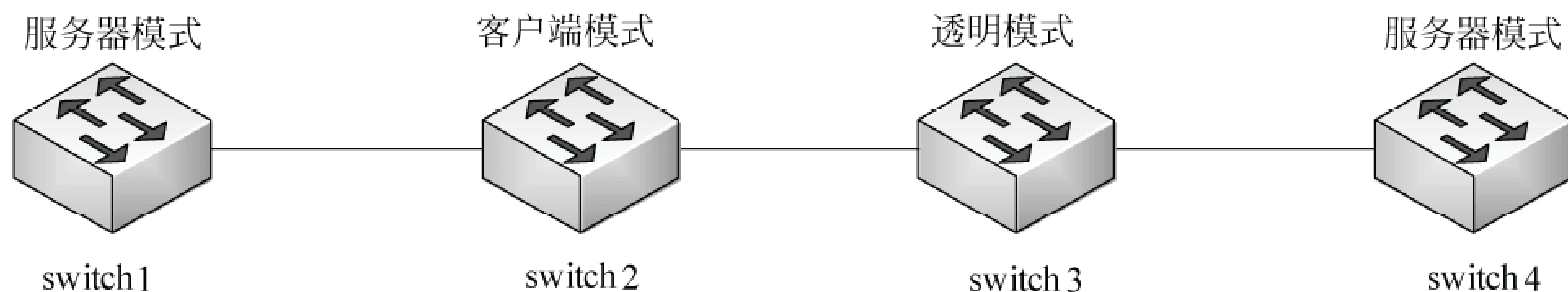
将多个子网断开后分别作为独立的网络进行测试，属于分段检查。既然断开就不可能是整体检查，而在断开子网的时候并没有分层或者按照 OSI 的参考模型来检测，另外断开子网并不是隔离网络。

参考答案

（68）C

试题（69）

某网络拓扑如下图所示，四个交换机通过中继链路互连，且被配置为使用 VTP，向 switch1 添加了一个新的 VLAN，__（69）__的操作不会发生。



（69）A．switch1 将 1 个 VTP 更新发送给 switch2

B．switch2 将该 VLAN 添加到数据库，并将更新发送给 switch3

C．switch3 将该 VTP 更新发送给 switch4

D．switch3 将该 VLAN 添加到数据库

试题（69）分析

本题考查 VTP 的基础知识。

VTP（VLAN Trunking Protocol）：是 VLAN 中继协议，也被称为虚拟局域网干道协议。它是思科私有协议。作用是十几台交换机在企业网中，配置 VLAN 工作量大，可以使用 VTP 协议，把一台交换机配置成 VTP Server, 其余交换机配置成 VTP Client，这样它们可以自动学习到 Server 上的 VLAN 信息。

VTP 有 3 种工作模式：VTP Server、VTP Client 和 VTP Transparent。新交换机出厂时的默认配置是预配置为 VLAN1，VTP 模式为服务器。一般，一个 VTP 域内的整个网络只设一个 VTP Server。VTP Server 维护该 VTP 域中所有 VLAN 信息列表，VTP Server 可以建立、删除或修改 VLAN，发送并转发相关的通告信息，同步 VLAN 配置，会把配置保存在 NVRAM 中。VTP Client 虽然也维护所有 VLAN 信息列表，但其 VLAN 的配置信息是从 VTP Server 学到的，VTP Client 不能建立、删除或修改 VLAN，但可以转发通告，同步 VLAN 配置，不保存配置到 NVRAM 中。VTP Transparent 相当于是一项独立的交换机，它不参与 VTP 工作，不从 VTP Server 学习 VLAN 的配置信息，而只拥有本设备上自己维护的 VLAN 信息。VTP Transparent 可以建立、删除和修改本机上的 VLAN 信息，同时会转发通告并把配置保存到 NVRAM 中。

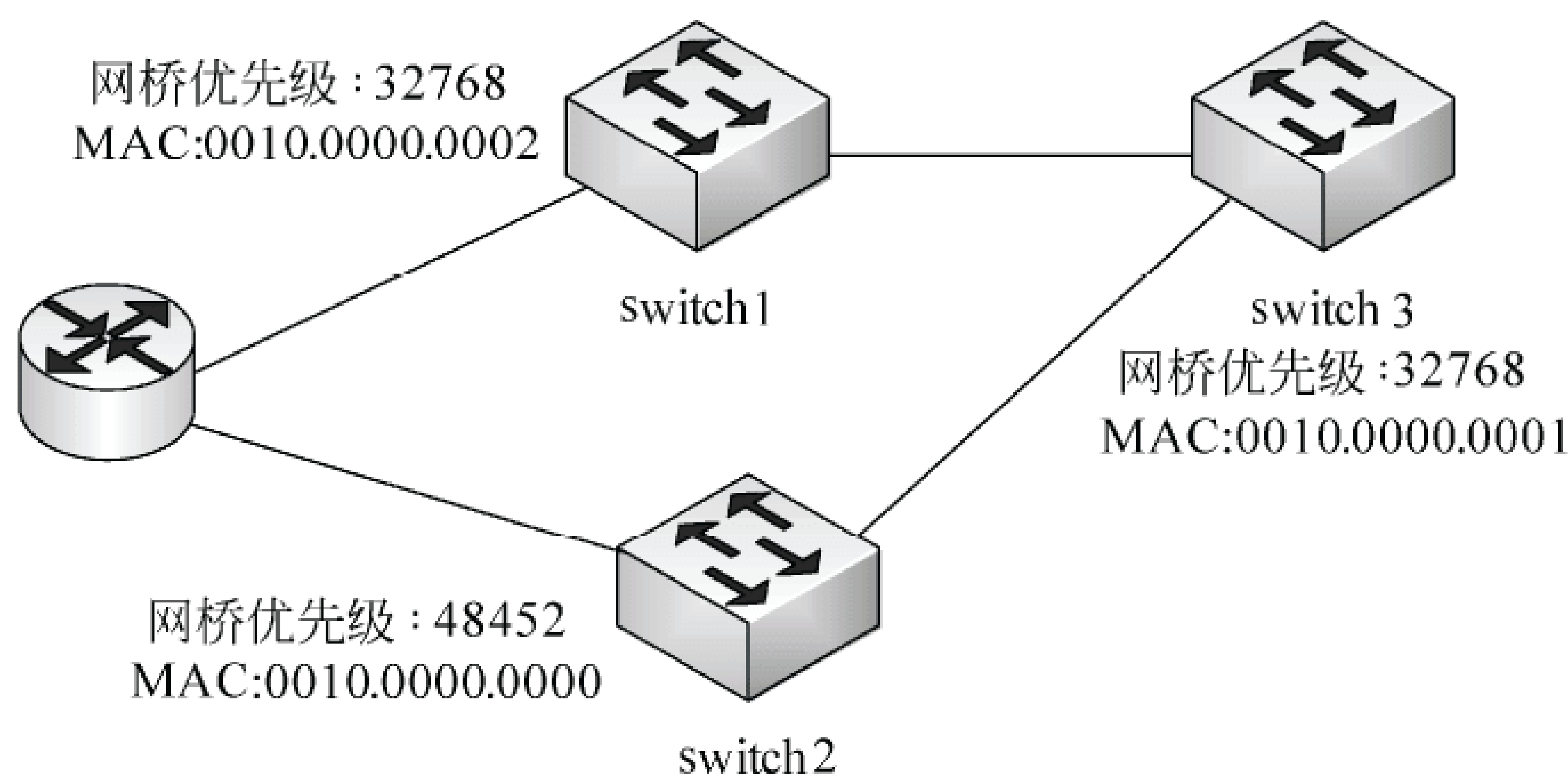
从图中可以看出，switch3 处于透明模式下，那么它将不会把自己的 VLAN 数据库与收到的通告同步，因此不会发生 switch3 将该 VLAN 添加到数据库的处理。

参考答案

（69）D

试题（70）

如下图，生成树根网桥选举的结果是＿（70）＿。



（70）　A．switch1 将成为根网桥

B．switch2 将成为根网桥

C．switch3 将成为根网桥

D．switch1 和 switch2 将成为根网桥

试题（70）分析

本题考查生成树根网桥的选举过程。

网桥 ID 是生成树算法所使用的第一个参数。STP 使用网桥 ID 来决定根网桥或者根交换机。网桥 ID 参数是 1 个 8 字节域，由一对有序数字组成。最开始的 2 字节的十进制数称为网桥优先级，接下来是 6 字节（十六进制）的 MAC 地址。网桥优先级是一个十进制数，用来在生成树算法中衡量一个网桥的优先度。其值的范围是 0-65535，默认设置为 32768。网桥 ID 中的 MAC 地址是交换机的 MAC 地址，每个交换机都有一个 MAC 地址池，每个 STP 实例使用一个作为 VLAN 生成树的实例的网桥 ID。

比较两个网桥 ID 的原则是：

① 首先比较网桥优先级，网桥优先级小的网桥 ID 优先；

② 如果两个网桥优先级相同，再比较 MAC 的地址，MAC 地址小的网桥 ID 优先。

根据上述原则，在上图中 Switch3 的网桥 ID 最小，则其优先为根网桥。

参考答案

（70）C

试题（71）～（75）

Symmetric, or private-key, encryption is based on a secret key that is shared by both communicating parties. The __(71)__ party uses the secret key as part of the mathematical operation to encrypt __(72)__ text to cipher text. The receiving party uses the same secret key to decrypt the cipher text to plain text. Asymmetric, or public-key, encryption uses two different keys for each user: one is a __(73)__ key known only to this one user; the other is a corresponding public key, which is accessible to anyone. The private and public keys are mathematically related by the encryption algorithm. One key is used for encryption and the other for decryption, depending on the nature of the communication service being implemented. In addition, public key encryption technologies allow digital __(74)__ to be placed on messages. A digital signature uses the sender's private key to encrypt some portion of the message. When the message is received, the receiver uses the sender's __(75)__ key to decipher the digital signature to verify the sender's identity.

（71）A．host B．terminal C．sending D．receiving

（72）A．plain B．cipher C．public D．private

（73）A．plain B．cipher C．public D．private

（74）A．interpretation B．signatures C．encryption D．decryption

（75）A．plain B．cipher C．public D．private

试题（71）～（75）翻译

对称加密或私钥加密的基础是通信双方共享同一密钥。发送方使用一个密钥作为数学运算的一部分把明文加密成密文。接收方使用同一密钥把密文解密变成明文。在非对称或公钥加密方法中，每个用户使用两种不同的密钥：一个是只有这个用户知道的私钥；另一个是与其对应的任何人都知道的公钥。根据加密算法，私钥和公钥是数学上相关的。一个密钥用于加密，而另一个用于解密，依赖于实现的通信服务的特点而用法有所不同。此外，公钥加密技术也可以用于报文的数字签名。数字签名时使用发送方的私钥来加密一部分报文。当接收方收到报文时，就用发送方的公钥来解密数字签名，以便对发送方的标识进行验证。

参考答案

（71）C　（72）A　（73）D　（74）B　（75）C

第 23 章　2015 下半年网络规划设计师下午试题 I 分析与解答

试题一（共 25 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业网络拓扑如图 1-1 所示。

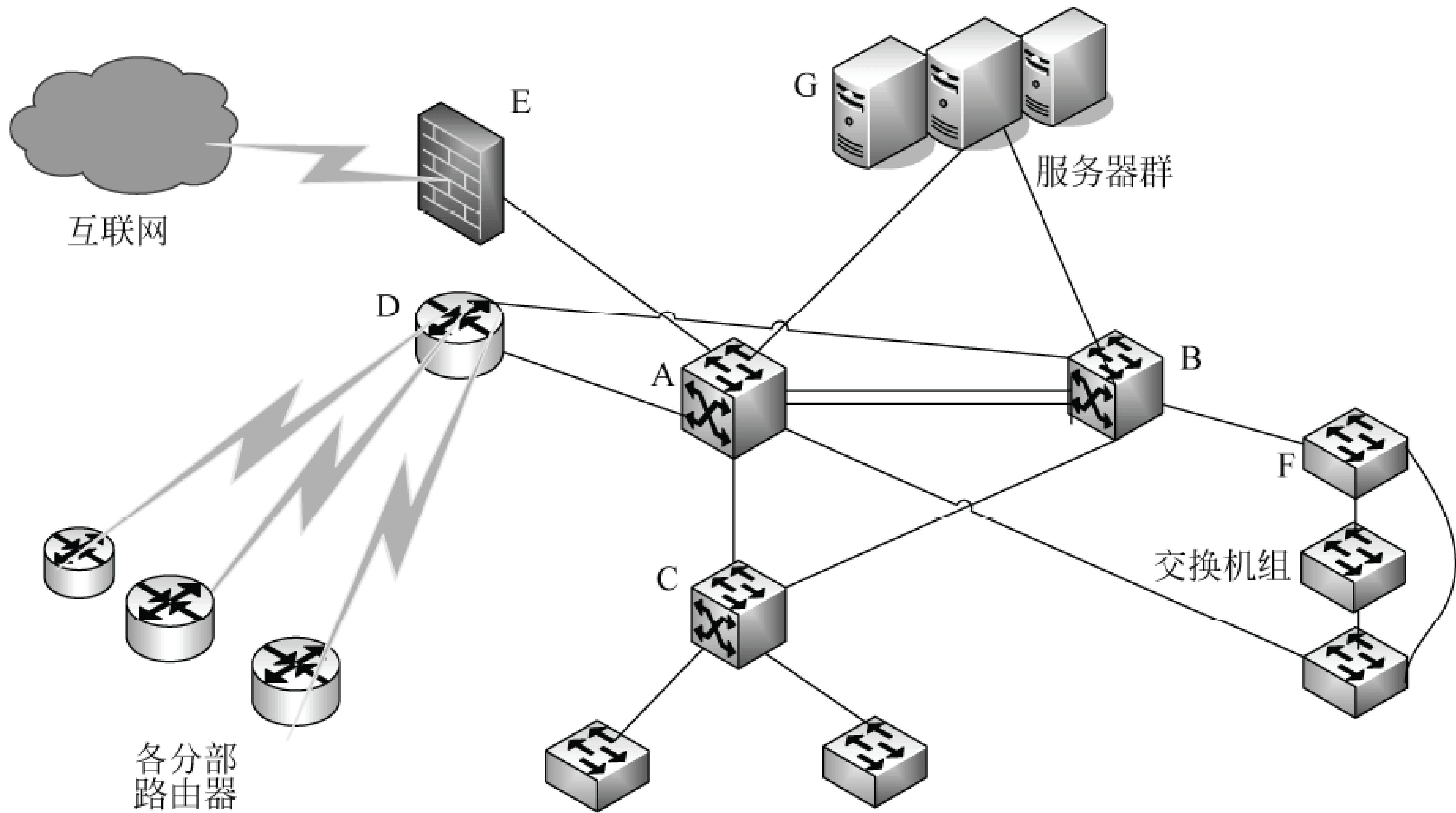


图 1-1

【问题 1】（6 分）

根据图 1-1，对该网络主要设备清单表 1-1 所示内容补充完整。

表 1-1

设备名	在网络中的编号	产品描述
Cisco6509	A，B	核心主、备交换机
Cisco4506	（1）	（2）
Ws-c3550-48	交换机组 F	接入层交换机
Cisco3745	（3）	（4）
Netscreen-500	（5）	（6）

【问题 2】（8 分）

1．网络中 A、B 设备连接的方式是什么？依据 A、B 设备性能及双链路连接，计算

两者之间的最大带宽。

2．交换机组 F 的连接方式是什么？采用这种连接方式的好处是什么？

【问题 3】（6 分）

该网络拓扑中连接到各分部可采用租赁 ISP 的 DDN、Frame Relay、ISDN 线路等方式，请简要介绍这几种连接方式。

【问题 4】（5 分）

若考虑到成本问题，对其中一条连接到分部的线路用 VPN 的方式，在分部路由器上做下列配置：

```
sub-company(config)#crypto isakmp policy 1
sub-company(config-isakmp)#encry des
sub-company(config-isakmp)#hash md5
sub-company(config-isakmp)#authentication pre-share
sub-company(config-isakmp)#exit
sub-company(config)#crypto isakmp key 6 cisco address x.x.x.x
```

该命令片段配置的是＿（7）＿。

（7）备选答案：

A．定义 ESP

B．IKE 策略

C．IPSce VPN 数据

D．路由映射

在该配置中，IP 地址 x.x.x.x 是该企业总部 IP 地址还是分部 IP 地址？

试题一分析

本题考查接入网技术和网络规划及配置的相关知识。

此类题目要求考生认真阅读题目或给出的网络拓扑图，对网络拓扑中采用组网技术进行分析说明。

【问题 1】

要求对组网设备的性能和功能分析，结合网络拓扑图和设备列表补充完善表格中的空白处。网络拓扑中没有在设备列表中标注的有 C、D、E、G 等设备。看图例可知 D、E 分别是路由器和防火墙，C 是介于 A、B 和 F 的交换机设备。根据 D、E、C 设备在网络中承担的任务，参照表中的产品描述，C 为汇聚交换机、D 为核心路由器、E 为核心路由器。

【问题 2】

网络中 A、B 设备连接的方式是链路聚合或捆绑。链路聚合是将两个或更多数据信道结合成一个单个的信道，该信道以一个单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。A、

B 设备可以配置千兆或者万兆的接口，在双链路聚合的前提下，最大带宽是 2G 或 20G。

交换机组 F 的连接方式是堆叠，堆叠需要专用的堆叠模块和堆叠线缆。堆叠可以扩大网络接入规模，对所有的交换机进行统一配置和管理，达到提高交换机背板容量，实现所有交换机高速连接的目的。

【问题 3】

DDN专线接入向用户提供的是永久性的数字连接，沿途不进行复杂的软件处理，因此延时较短，避免了传统的分组网中传输协议复杂、传输时延长且不固定的缺点；DDN 专线接入采用交叉连接装置，可根据用户需要，在约定的时间内接通所需带宽的线路，信道容量的分配和接续均在计算机控制下进行，具有极大的灵活性和可靠性，使用户可以开通各种信息业务，传输任何合适的信息。

帧中继是一种局域网互联的 WAN 协议，它工作在 OSI 参考模型的物理层和数据链路层。它为跨越多个交换机和路由器的用户设备间的信息传输提供了快速和有效的方法。帧中继是一种数据包交换技术，与 X.25 类似。它可以使终端站动态共享网络介质和可用带宽。

ISDN 综合业务数字网（Integrated Services Digital Network）是一个数字电话网络国际标准，是一种典型的电路交换网络系统。在 ITU 的建议中，ISDN 是一种在数字电话网 IDN 的基础上发展起来的通信网络，ISDN 能够支持多种业务，包括电话业务和非电话业务。

【问题 4】

采用 VPN 连接，网络对等端需要建立信任关系，必须交换某种形式的认证密钥。Internet 密钥交换(Internet Key Exchange，IKE)是一种为 IPSec 管理和交换密钥的标准方法。该过程一般包括定义策略、定义加密算法、定义散列算法、定义认证方式等步骤。

在分部路由器上配置 IKE 策略，x.x.x.x 是对端地址。

试题一参考答案

【问题 1】

（1）C

（2）汇聚交换机

（3）D

（4）核心路由器

（5）E

（6）边界防火墙

【问题 2】

1. 链路聚合或捆绑

   2G（或答 20G 也正确）

2．堆叠

扩大接入规模，简化网络管理

【问题 3】

DDN 是利用数字信道提供永久性连接电路，用来传输数据信号的数字传输网络。

帧中继是一种数据包交换技术，可以动态共享网络介质和可用带宽。

ISDN 是一个数字电话网络标准，是一种典型的电路交换网络系统。

【问题 4】

（7）B

总部 IP 地址

试题二（共 25 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

传统业务结构下，由于多种技术之间的孤立性，使得数据中心服务器总是提供多个对外 I/O 接口。在云计算模式发展的推动下，数据中心正在从过去的存储处理中心演变成为应用中心，并逐步向服务中心和运营中心转变。而对客户来说，由于技术，经验，资金等限制，在转变过程中会遇到各种挑战，例如：虚拟化带来的技术复杂性，规模扩大带来的运维压力，系统和数据迁移的困难以及数据中心的高能耗等。

传统业务结构下的数据中心网拓扑结构图如图 2-1 所示。

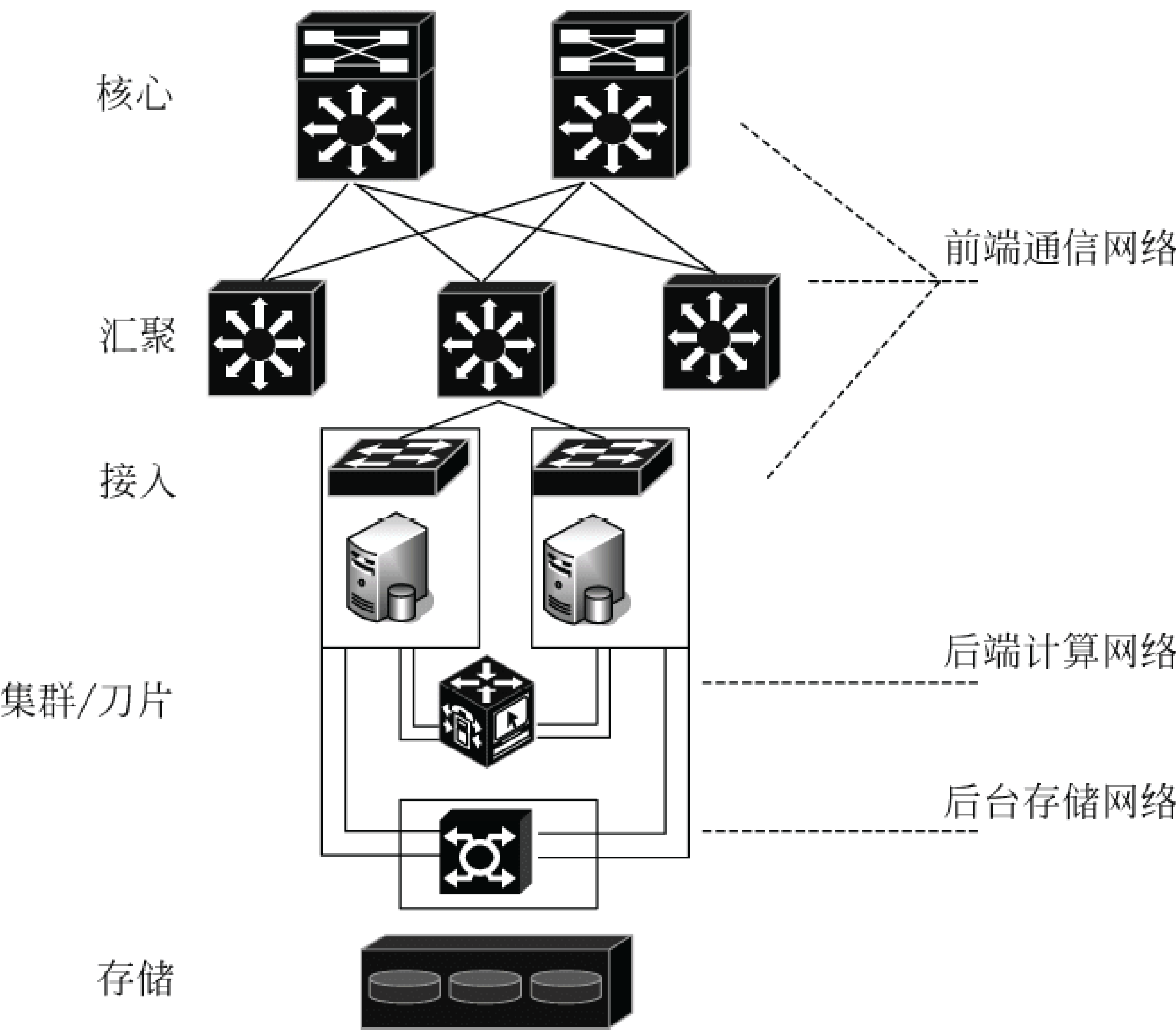


图 2-1

【问题 1】（9 分）

（1）如图 2-1 所示，数据中心有多个网络，一个是前端用户通信网络，一个是后端

做数据更新或者做集群计算的通讯网络，还有后台光纤存储网络。针对这 3 种网络分别举出一个例子。

（2）如上所述，除以上 3 种网络外，有的数据中心还有专门用于虚拟机迁移的网络，都会在服务器上做集中。这样一台服务器最多需要几块网卡与之相连？随着 TRILL 等技术的出现，这个专用网络还需要吗？

（3）网络成为数据中心资源的交换枢纽，当前数据中心分为 IP 数据网络、存储网络、服务器集群网络。随着数据中心规模的逐步增大，简单分析带来的问题。

【问题 2】（4 分）

FCoE 采用增强型以太网作为物理网络传输架构，是专门为低延迟性、高性能、二层数据中心网络所设计的网络协议。目前国际标准化组织已经开发了针对以太网标准的扩展协议族，即“融合型增强以太网（CEE）”，这些扩展协议族可以进行所有类型的传输。试简述 FCoE 技术的优点。

【问题 3】（6 分）

为了实现统一管理、简化运维，采用基于 FCoE 技术的数据中心统一 I/O 能够实现用少数的 CNA（Converged Network adapter）代替数量较多的 NIC、HBA、HCA，所有的流量通过 CNA 万兆以太网传输。

按照 18 台服务器（单网卡）为例，使用 FCoE 后每台服务器只需要一块专用适配器（网卡），一套布线（以太网）系统，统一管理维护简单。表 2-1 为使用 FCoE 前 18 台服务器需要的网卡、交换机、电缆以及上联端口的数量；请核算出使用 FCoE 后的相应部件数量，填充表 2-2。

表 2-1 使用 FCoE 前

18 台服务器	Ethernet	FC	合计
网卡	18	18	36
交换机	2	2	4
电缆	36	36	72
上联端口	2	4	6

表 2-2 使用 FCoE 后

18 台服务器	CEE	Ethernet	FC	合计
网卡	18	（1）	（5）	（9）
交换机	2	（2）	（6）	（10）
电缆	36	（3）	（7）	（11）
上联端口	2	（4）	（8）	（12）

【问题 4】（6 分）

（1）随着数据中心的发展，数据中心的能耗已经成为一个严峻的问题，PUE 值已经

成为国际上比较通行的数据中心电力使用效率的衡量指标。请问 PUE 是什么，它的基准是多少，其越接近多少表示一个数据中心的绿色化程度越高？

（2）在现代机房的机柜布局中，人们为了美观和便于观察会将所有的机柜朝同一个方向摆放。如果按照这种摆放方式，机柜盲板有效阻挡冷热空气的效果将大打折扣。正确的摆放方式是什么？请简述其原因。

（3）水冷空调系统是目前新一代大型数据中心制冷的首选方案，采用水冷空调在部分地区可以采取免费冷却技术以节能。免费冷却技术是什么？

试题二解析

本题考查云计算模式下的数据中心的相关知识及应用。

【问题 1】

本问题主要考查传统数据中心的问题及 I/O 融合趋势。

传统业务结构下，由于多种技术之间的孤立性（LAN 与 SAN），使得数据中心服务器总是提供多个对外 I/O 接口（在此，可理解成服务器的网卡），即用于数据计算与交互的 LAN 接口以及数据访问的存储接口，某些特殊环境如特定 HPC（高性能计算）环境下的超低时延接口。服务器的多个 I/O 接口导致了数据中心环境下多个独立运行的网络同时存在，不仅使得数据中心布线复杂，不同的网络、接口形体造成的异构还直接增加了额外人员的运行维护、培训管理等高昂成本投入，特别是存储网络的低兼容性特点，使得数据中心的业务扩展往往存在约束。

数据中心里会有两个网络，一个是前端 IP 网络，后端可能会是光纤网络，都会在服务器上做。因此，集中服务器上以太网卡、光纤网卡，跟外部数据交互时通过 IP 网络进行交互。如果说得更极端一点，在大型数据中心会存在：一是前端的用户通信网络（以太网）；二是后台存储网络光纤的通道（FC 光纤网络）；三是后端做数据更新或者做集群计算的通信网络（高性能计算 Infiniband 网络）；四是专门用于虚拟机迁移的网络（各个服务器上有一个普通的以太网网卡，连接到独立的交换机组成的网络上，专门做虚拟机迁移。随着 TRILL 等技术的出现，这个专用的网络不再需要）。在这种情况下最多会有八个网卡，这些都是现有的设计视为理所当然的。

网络渐渐成为数据中心资源的交换枢纽。当前数据中心分为 IP 数据网络、存储网络、服务器集群网络。但随着数据中心规模的逐步增大，也带来以下问题：每个服务器要多个专用适配器（网卡），要有不同的布线系统；机房要支持更多设备：空间、耗电、制冷；多套网络无法统一管理，不同的维护人员；部署/配置/管理/运维困难。

【问题 2】

FCoE 采用增强型以太网作为物理网络传输架构，能够提供标准的光纤通道有效内容载荷，避免了 TCP/IP 协议开销，而且 FCoE 能够像标准的光纤通道那样为上层软件层

（包括操作系统、应用程序和管理工具）服务。

FCoE 可以提供多种光纤通道服务，比如发现、全局名称命名、分区等，而且这些服务都可以像标准的光纤通道那样运作。不过，由于 FCoE 不使用 TCP/IP 协议，因此 FCoE 数据传输不能使用 IP 网络。FCoE 是专门为低延迟性、高性能、二层数据中心网络所设计的网络协议。

和标准的光纤通道 FC 一样，FCoE 协议也要求底层的物理传输是无损失的。因此，国际标准化组织已经开发了针对以太网标准的扩展协议族，尤其是针对无损 10Gb 以太网的速度和数据中心架构。这些扩展协议族可以进行所有类型的传输。这些针对以太网标准的扩展协议族被国际标准组织称为“融合型增强以太网（CEE）”（思科称为“数据中心以太网（DCE）”）。

数据中心 FCoE（FC over Ethernet）技术实现在以太网架构上映射 FC（Fibre Channel）帧，使得 FC 运行在一个无损的数据中心以太网络上（需要无损的以太网（CEE/DCE/DCB）保证不丢包）。FCoE 技术有以下的一些优点：光纤存储和以太网共享同一个端口；更少的线缆和适配器；软件配置 I/O；与现有的 SAN 环境可以互操作。

基于 FCoE 技术的数据中心统一 I/O 能够实现用少数的 CNA（Converged Network Adapter）代替数量较多的 NIC、HBA、HCA，所有的流量通过 CNA 万兆以太网传输。

使用 FCoE 后的好处：每个服务器只需要一个专用适配器（网卡），一套布线（以太网）系统（以前需要多个网卡，多套布线（以太网和光纤）系统）；机房不再要支持更多设备：空间、耗电、制冷，更加节能绿色；只有一套网络，统一管理维护简单（原来是多套网络无法统一管理，不同的维护人员维护困难）；部署/配置/管理/运维简单。

【问题 3】

使用前（按照 18 台服务器为例，如下表）

表 2-1 使用 FCoE 前

18 台服务器	Ethernet	FC	合计
网卡	18	18	36
交换机	2	2	4
电缆	36	36	72
上联端口	2	4	6

1．72 根光纤、36 个网卡（36 根以太网光纤、36 个以太网网卡，18 根 FC 光纤、18 个 FC 光纤网卡）。

2．4 台交换机（2 台以太网交换机，2 台 FC 光纤交换机）。

3．上联端口（6 个，以太网交换机要 2 个，光纤交换机需要 4 个）。

使用后（按照 18 台服务器为例，如下表）

表 2-2 使用 FCoE 后

18 台服务器	CEE	Ethernet	FC	合计
网卡	18	0	0	18
交换机	2	0	0	2
电缆	36	0	0	36
上联端口	2	0	4	6

1．36 根光纤、18 个网卡（36 根光纤、18 个 CNA 网卡）。

2．2 台交换机（2 台 FCoE 交换机）。

3．上联端口（6 个，以太网交换机要 2 个，光纤交换机需要 4 个）。

【问题 4】

本问题主要考查数据中心能耗的相关知识。

随着能源成本上升，我们越来越关注 IT 对环境的影响，技术管理人员现在面临着双重任务：创造和保持高可用性的 IT 环境，并推行绿色倡议。用于数据中心保证设备运行的能源消耗需求惊人。

（1）PUE 是 Power Usage Effectiveness 的简写，是评价数据中心能源效率的指标，是数据中心消耗的所有能源与 IT 负载使用的能源之比，是 DCIE（Data Center Infrastructure Efficiency）的反比。PUE = 数据中心总设备能耗/IT 设备能耗，PUE 是一个比值，基准是 2，越接近 1 表明能效水平越好。PUE（PowerUsageEffectiveness，电源使用效率）值已经成为国际上比较通行的数据中心电力使用效率的衡量指标。PUE 值是指数据中心消耗的所有能源与 IT 负载消耗的能源之比。PUE 值越接近于 1，表示一个数据中心的绿色化程度越高。

（2）以往在机柜的布局中，人们为了美观和便于观察，常常会将所有的机柜朝同一个方向摆放。如果按照这种摆放方式，机柜盲板有效阻挡冷热空气的效果将大打折扣。正确的摆放方式应该是将服务器机柜面对面或背对背的摆放方式摆放，这样便形成了冷风通道和热风通道，机柜之间的冷热风不会混合在一起，形成短路气流，有效提高制冷效果，保护好冷热通道不被破坏。即当机柜内或机架上的设备为前进风/后出风方式冷却时，机柜或机架的布置宜采用面对面、背对背方式。

（3）水冷式空调的发明源于生活的细节，夏季人站在海边感觉特别凉爽，这是因为海水吸收空气中的热量而蒸发，使空气温度下降，从而带给我们凉爽的冷空气。细心的人们发现了这一现象，并将这一现象巧妙地运用到温度调节中来，进而发明了节能环保的水冷空调。水冷空调又叫环保空调，是一种利用自来水的温度，来达到冷却室内温度的空调机。

水冷空调系统是目前新一代大型数据中心制冷的首选方案，采用水冷空调在部分地区可以采取免费冷却技术以节能。免费冷却技术指全部或部分使用自然界的免费冷源进

行制冷从而减少压缩机或冷冻机消耗的能量。目前常用的免费冷源主要是冬季或者春秋季的室外空气，因此，如果可能的话，数据中心的选址应该在天气比较寒冷或低温时间比较长的地区。在中国，北方地区都是非常适合采用免费制冷技术。

试题二参考答案

【问题 1】

（1）前端：以太网

后端：高性能计算 Infiniband 网络

后台：FC 光纤

（2）8 个网卡

不需要

（3）每个服务器要多个专用适配器（网卡）以及不同的布线系统；

机房要支持更多设备；

管理的复杂性增加；

部署/配置/运维困难；

成本增加（人员，能耗，运维成本等）。

【问题 2】

光纤存储和以太网共享同一个端口；

更少的线缆和适配器；

软件配置 I/O；

与现有的 SAN 环境可以互操作。

【问题 3】

（1）0 （2）0 （3）0 （4）0 （5）0 （6）0

（7）0 （8）4 （9）18 （10）2 （11）36 （12）6

【问题 4】

（1）PUE ＝ 数据中心总设备能耗/IT 设备能耗，基准是 2，越接近 1 表明能效水平越好。

（2）将服务器机柜面对面或背对背的方式摆放。

因为这样将会形成“冷”通道和“热”通道，提高制冷效果。

（3）免费冷却（Free Cooling）技术指全部或部分使用自然界的免费冷源进行制冷从而减少压缩机或冷冻机消耗的能量。

试题三（25 分）

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某学校拥有内部数据库服务器 1 台，邮件服务器 1 台，DHCP 服务器 1 台，FTP 服务器 1 台，流媒体服务器 1 台，Web 服务器 1 台。要求为所有的学生宿舍提供有线网络

接入服务，对外提供 Web 服务、邮件服务、流媒体服务，内部主机和其他服务器对外不可见。

【问题 1】（5 分）

请划分防火墙的安全区域，说明每个区域的安全级别，指出各台服务器所处的安全区域。

【问题 2】（5 分）

请按照你的思路为该校进行服务器和防火墙部署设计，对该校网络进行规划，画出网络拓扑结构图。

【问题 3】（5 分）

学校在原有校园网络基础上进行了扩建，采用 DHCP 服务器动态分配 IP 地址。运行一段时间后，网络时常出现连接不稳定、用户所使用的 IP 地址被“莫名其妙”修改、无法访问校园网的现象。经检测发现网络中出现多个未授权 DHCP 地址。

请分析上述现象及遭受攻击的原理，该如何防范？

【问题 4】（6 分）

学生宿舍区经常使用的服务有 Web、即时通信、邮件、FTP 等，同时也因视频流导致大量的 P2P 流量，为了保障该区域中各项服务均能正常使用，应采用何种设备合理分配每种应用的带宽？该设备部署在学校网络中的什么位置？一般采用何种方式接入网络？

【问题 5】（4 分）

当前防火墙中，大多都集成了 IPS 服务，提供防火墙与 IPS 的联动。区别于 IDS，IPS 主要增加了什么功能？通常采用何种方式接入网络？

试题三分析

本题考查局域网安全部署的基本知识及应用。

【问题 1】

根据题目中关于该学校所拥有的服务器类型和服务器数量、基本要求以及服务器对用户的访问权限等说明，考虑到防火墙的 3 种区域划分，可将网络分为内部网络、外部网络和 DMZ 区 3 个区域，这 3 个区域中，内部网络的安全要求级别最高，DMZ 区次之，外部网络的安全要求级别最高。

【问题 2】

根据问题 1 对该学校网络区域的划分，将不同的服务器放置在相应的区域即可，对于具体的网络连接细节则不必过多地考虑，在防火墙的 DMZ 区中，由于需要连接多台服务器，应使用一台局域网交换机进行连接。

【问题 3】

当采用 DHCP 服务器为客户端动态分配 IP 地址时，出现网络连接不稳定、用户的地址会被“莫名其妙”修改，导致无法访问校园网的现象，经查是出现了多个未授权的

DHCP 服务器所致。这些所谓“未授权”的服务器为客户机分配了其他的非法 IP 地址，导致用户无法访问网络。这类攻击为 DHCP 攻击，DHCP 攻击的原理是距离客户端较近的 DHCP 服务器会先于授权 DHCP 服务器相应客户端的请求，而导致客户端接收到非法 IP 地址，无法访问网络。防范的方法一般是在接入层交换机上启用 DHCP Snooping 功能，以过滤非信任接口上收到的 DHCP offer、DHCP ACK 和 DHCPNCK 报文，从而防止非法的 DHCP 服务器为客户端分配 IP 地址。

【问题 4】

根据问题的描述，由于网络中存在大量的 P2P 流量，而导致其他各项服务正常工作，应对 P2P 流量进行控制。要实现该功能，一般所选用的设备为流控设备，流控设备一般部署在被控流量区域的主干区域，应采用串接方式接入网络。

【问题 5】

随着网络攻击技术的发展，对安全技术提出了新的挑战。防火墙技术和 IDS 自身具有的缺陷阻止了它们进一步的发展。防火墙不能阻止内部网络的攻击，对于网络上流行的各种病毒也没有很好的防御措施；IDS 只能检测入侵而不能实时地阻止攻击，而且 IDS 具有较高的漏报和误报率。

在这种情况下入侵防御系统（Intrusion Prevention System，IPS）成了新一代的网络安全技术。IPS 提供主动、实时的防护，其设计旨在对网络流量中的恶意数据包进行检测，对攻击性的流量进行自动拦截，使它们无法造成损失。IPS 如果检测到攻击企图，就会自动地将攻击包丢掉或采取措施阻断攻击源，而不把攻击流量放进内部网络。

IPS 和 IDS 的部署方式不同。串接式部署是 IPS 和 IDS 区别的主要特征。IDS 产品在网络中是旁路式工作，IPS 产品在网络中是串接式工作。串接式工作保证所有网络数据都经过 IPS 设备，IPS 检测数据流中的恶意代码，核对策略，在未转发到服务器之前，将信息包或数据流拦截。由于是在线操作，因而能保证处理方法适当而且可预知。

IPS 系统根据部署方式可以分为 3 类：基于主机的入侵防护（HIPS）、基于网络的入侵防护（NIPS）、应用入侵防护（AIP）。

试题三参考答案

【问题 1】

整个网络分为 3 个不同级别的安全区域：

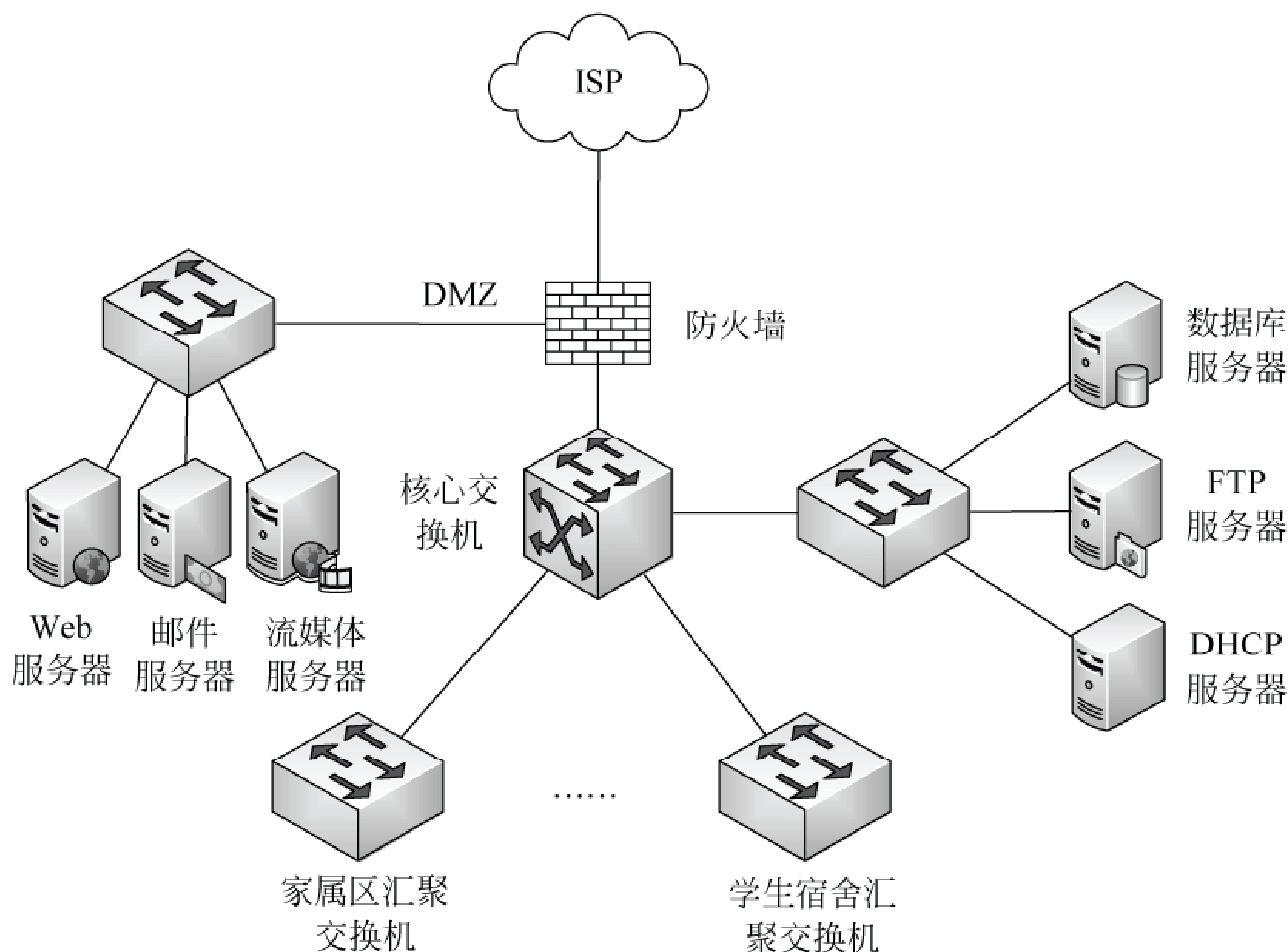
1．内部网络：安全级别最高，是可信的、重点保护的区域。包括所有内部主机，数据库服务器、DHCP 服务器和 FTP 服务器。

2．外部网络：安全级别最低，是不可信的、要防备的区域。包括外部因特网用户主机和设备。

3．DMZ 区域（非军事化区）：安全级别中等，因为需要对外开放某些特定的服务和应用，受一定的保护，是安全级别较低的区域。包括对外提供 WWW 访问的 Web 服务器、邮件服务器和流媒体服务器。

【问题 2】

拓扑结构图如下：



注：1. DMZ 区服务器群，内网服务器群放置位置，防火墙位置，网络层次结构，学生宿舍汇聚接入。

2. 合理的服务器放置和防火墙配置也正确，比如出口防火墙采用端口映射来区别是否为外网提供服务。

【问题 3】

攻击原理：

（1）当 DHCP 客户端第一次连接网络、重新连接或者地址租期已满时，会以广播的方式向 DHCP 服务器发送 DHCP Discover 消息，以获取/重新获取 IP 地址；

（2）若网络中存在多台 DHCP 服务器，均能收到该消息并应答；

（3）非授权 DHCP 服务器会先于授权 DHCP 服务器发出应答；

（4）客户端使用非授权服务器发出的应答包，并用作自己的 IP 地址；

（5）客户端地址被修改，无法访问校园网。

防范措施：

（1）启用接入层交换机的 DHCP Snooping 功能；

（2）DHCP Snooping 功能将交换机接口分为信任接口和非信任接口；

（3）连接客户端的接口为非信任接口，上连到汇聚交换机的接口为信任接口；

（4）非信任接口上接收到 DHCP Offer、DHCP ACK、DHCPNCK 报文时，交换机会

将其丢弃；

（5）DHCP Snooping 功能可阻止连接在非信任接口上的非授权 DHCP 服务器为客户端提供 IP 地址配置信息。

【问题 4】

应采用流量控制设备，部署在核心交换机与学生宿舍区汇聚交换机之间，采用串接方式接入网络。

【问题 5】

区别于 IDS，IPS 提供主动防护，增加了深入检测和分析功能，提供高效处理（拦截或阻断）能力。采用串接方式接入网络。

第 24 章　2015 下半年网络规划设计师下午试题 II 写作要点

论题一　局域网络中信息安全方案设计及攻击防范技术

信息化的发展与信息安全保障是密切相关的，两者相辅相成、密不可分。信息安全在国家安全中占有极其重要的战略地位，已经成为国家安全的基石和核心，并迅速渗透到国家的政治、经济、文化、军事安全中去，成为影响政治安全的重要因素。

（请围绕“局域网络中信息安全方案设计及攻击防范技术”论题，依次对以下四个方面进行论述。）

1．简要论述你参与建设的局域网络环境及建立在网络之上的业务。

2．详细论述局域网络中信息安全涉及到的主要问题及相应防范技术。

3．详细论述你参与设计和实施的网络项目中采用的安全方案。

4．分析所采用方案遵循的原则，评估安全防范方案的效果以及进一步改进的措施。

写作要点：

1．简要论述安全方案遵循标准及分级。

2．简要介绍局域网络环境拓扑结构，分层模型。

3．简要介绍公司网络业务，安全需求分析。

4．详细论述局域网络层次架构中各层遇到的安全问题及如何设计防范措施。

5．详细论述你采用的安全方案。

6．对安全方案进行评估。

7．介绍实际运行过程中安全防范方案出现的问题，如何解决，方案上有何改进措施。

论题二　智能小区 WIFI 覆盖解决方案

WIFI 使用无线传输介质，是实现移动计算机网络的关键技术之一。智能小区规划与设计常用的无线接入解决方案，是对有线网络接入方式的一种补充。目前，WIFI 网络已经成为人们日常生活中不可或缺的组成部分。

（请围绕“智能小区 WIFI 覆盖解决方案”论题，依次对以下四个方面进行论述。）

1．概述 WLAN 的通信技术、体系结构、工业标准，以及安全措施。

2．简要阐述你参与建设的智能小区无线网络的需求分析。

3．根据需求详细论述你参与设计和实施的无线网络组网方案，包括中心机房、有线骨干网、有线/无线中间层、节点交换机，无线接入点的分布，网络拓扑结构图和无线覆盖效果图，用户认证、访问控制和计费管理，AP 的控制和管理等。

4．分析你在网络建设和管理过程中遇到的问题，评估安全防范方案的效果以及进

一步改进的措施。

写作要点：

1．概述 WLAN 的通信技术、体系结构、工业标准，以及安全措施。

2．园区无线网络建设的需求分析。

3．根据需求导出的组网方案：

- 中心机房；
- 有线骨干网、有线/无线中间层、节点交换机；
- 无线接入点的分布（频率规划，覆盖方式，室内/外设备的选型、安装和供电）；
- 网络拓扑结构图和无线覆盖效果图；
- 用户认证、访问控制和计费管理（802.1x、PPPoE 和 Web 认证，AAA 和 Radius）；
- AP 的控制和管理。

4．网络建设和管理过程中问题：

- 流量监测及报警；
- 安全管理和防雷电措施；
- 漫游切换；
- 可扩展性。